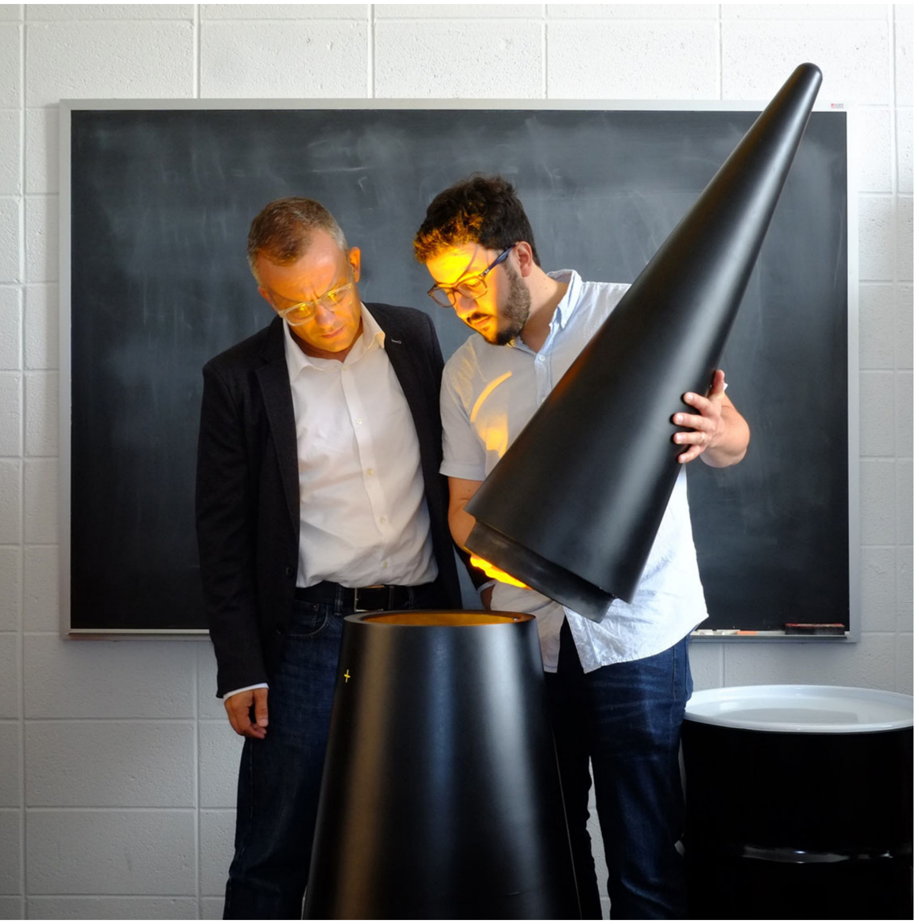


HOW I LEARNED TO STOP WORRYING AND DISMANTLE THE BOMB

NEW APPROACHES TO NUCLEAR WARHEAD VERIFICATION

Alex Glaser,* Sébastien Philippe,* and Robert J. Goldston**

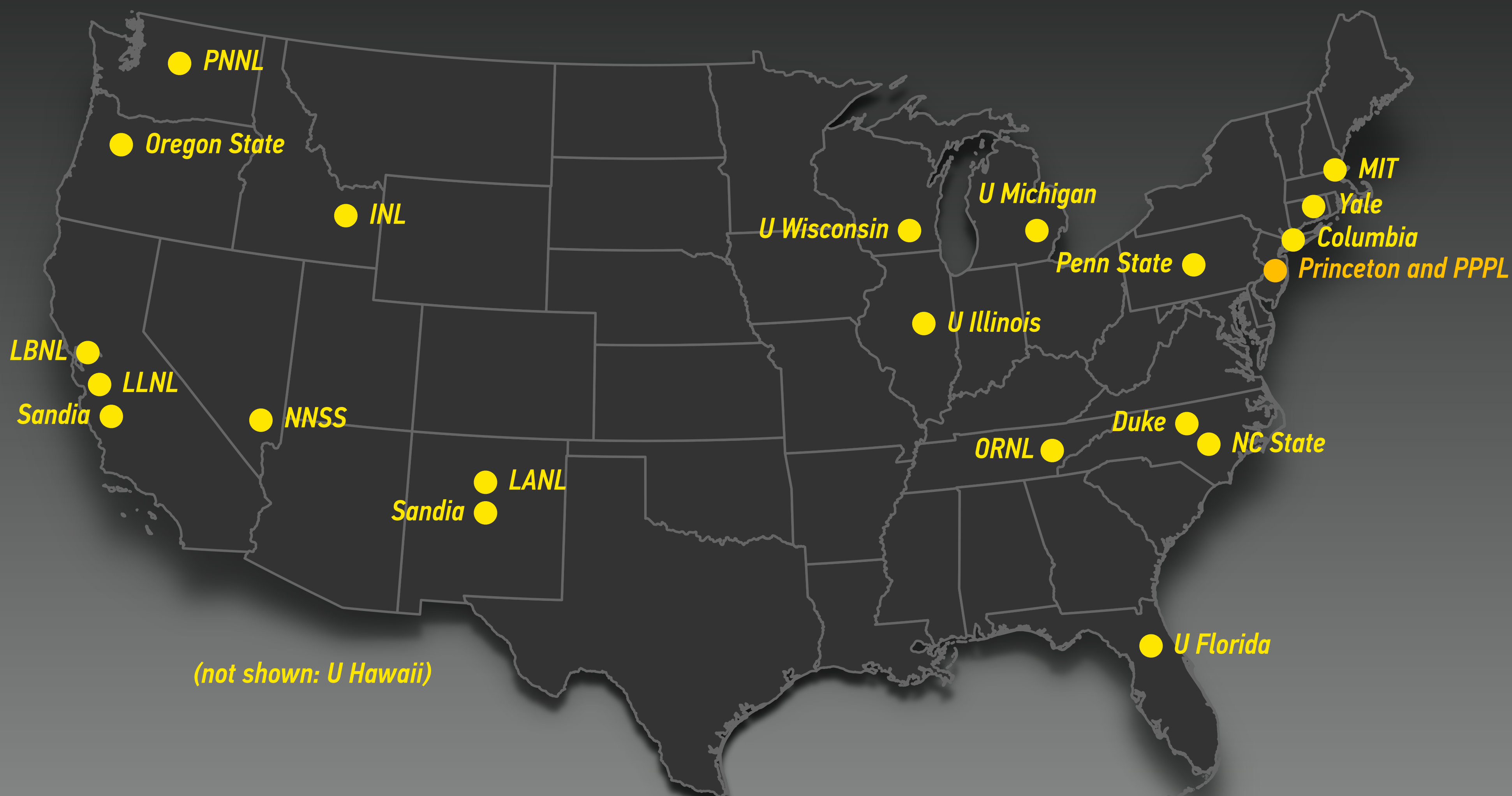
*Princeton University

**Princeton University and Princeton Plasma Physics Laboratory

Duke University, January 19, 2017

Revision 1

CONSORTIUM FOR VERIFICATION TECHNOLOGY



Five-year project, funded by U.S. DOE, 13 U.S. universities and 9 national labs, led by U-MICH

Princeton participates in the research thrust on disarmament research
(and leads the research thrust of the consortium on policy)

INTERNATIONAL PARTNERSHIP

FOR NUCLEAR DISARMAMENT VERIFICATION

Established in 2015; currently 26 participating countries

Working Group One: “Monitoring and Verification Objectives” (chaired by Italy and the Netherlands)
Working Group Two: “On-Site Inspections” (chaired by Australia and Poland)
Working Group Three: “Technical Challenges and Solutions” (chaired by Sweden and the United States)

www.state.gov/t/avc/ipndv

WHAT'S NEXT FOR NUCLEAR ARMS CONTROL ?

2015 STATEMENT BY JAMES MATTIS

"The nuclear stockpile must be tended to and fundamental questions must be asked and answered:

- *We must clearly establish the role of our nuclear weapons: do they serve solely to deter nuclear war? If so we should say so, and the resulting clarity will help to determine the number we need.*
- *Is it time to reduce the Triad to a Diad, removing the land-based missiles? This would reduce the false alarm danger.*
- *Could we re–energize the arms control effort by only counting warheads vice launchers?*
- *Was the Russian test violating the INF treaty simply a blunder or a change in policy, and what is our appropriate response?"*

General James N. Mattis, USMC (Ret.)
Former Commander, United States Central Command

Senate Armed Services Committee
Global Challenges and U.S. National Security Strategy
January 27, 2015

WHAT IS TO BE VERIFIED?

WHAT IS TO BE VERIFIED?

SELECTED CURRENT AND EMERGING VERIFICATION CHALLENGES FOR NUCLEAR ARMS CONTROL AND NONPROLIFERATION

1. VERIFYING NUMERICAL LIMITS OF DECLARED NUCLEAR WARHEADS

Requires techniques to account for (and identify) nuclear warheads in storage

for example, using (hashed) declarations, special tags, and/or unique identifiers (UIDs)

2. CONFIRMING THE AUTHENTICITY OF NUCLEAR WARHEADS

Requires dedicated inspection systems

for example, based on radiation-detection techniques (passive/active, neutron/gamma)

3. ESTABLISHING CONFIDENCE IN THE ABSENCE OF UNDECLARED STOCKS OR PRODUCTION

How to make sure that no covert warheads / materials exist outside the verification regime?

No silver bullet; but not much different from existing NPT verification challenges

Source: Paul Shambroom (top), Google Earth (middle), and U.S. Department of Energy (bottom)

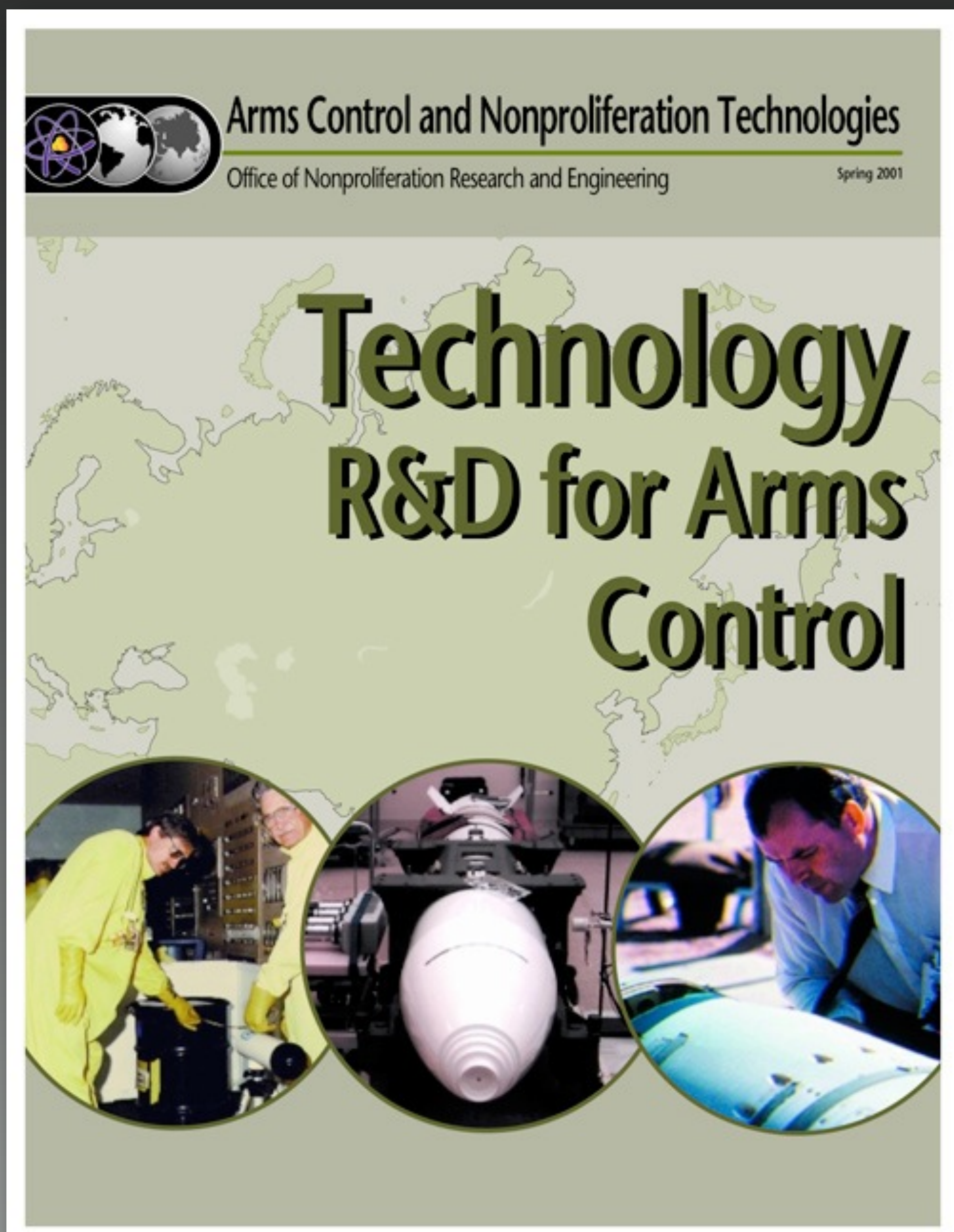
THOUSANDS OF NUCLEAR WEAPONS

ARE CURRENTLY NON-DEPLOYED (i.e., IN RESERVE OR AWAITING DISMANTLEMENT)

W87/Mk-21 Reentry Vehicles in storage, Warren Air Force Base, Cheyenne, Wyoming
Photo courtesy of Paul Shambroom, www.paulshambroom.com

NUCLEAR WARHEAD VERIFICATION

KEY CONCEPTS OF (PROPOSED) SYSTEMS



edited by D. Spears, 2001

ATTRIBUTE APPROACH

Confirming selected characteristics
of an object in classified form
(for example, the presence/mass of plutonium)

TEMPLATE APPROACH

Comparing the radiation signature
from the inspected item with a reference item
("golden warhead") of the same type

INFORMATION BARRIERS

Technologies and procedures that
prevent the release of sensitive nuclear information
(generally needed for both approaches)

PREVENTING THE EXCHANGE OF SENSITIVE INFORMATION DURING A RADIATION MEASUREMENT

Trusted Information Barrier

Measure (but sanitize) sensitive information

"Hard" to authenticate and certify

Single-bit observation

Interactive Zero-knowledge Proof

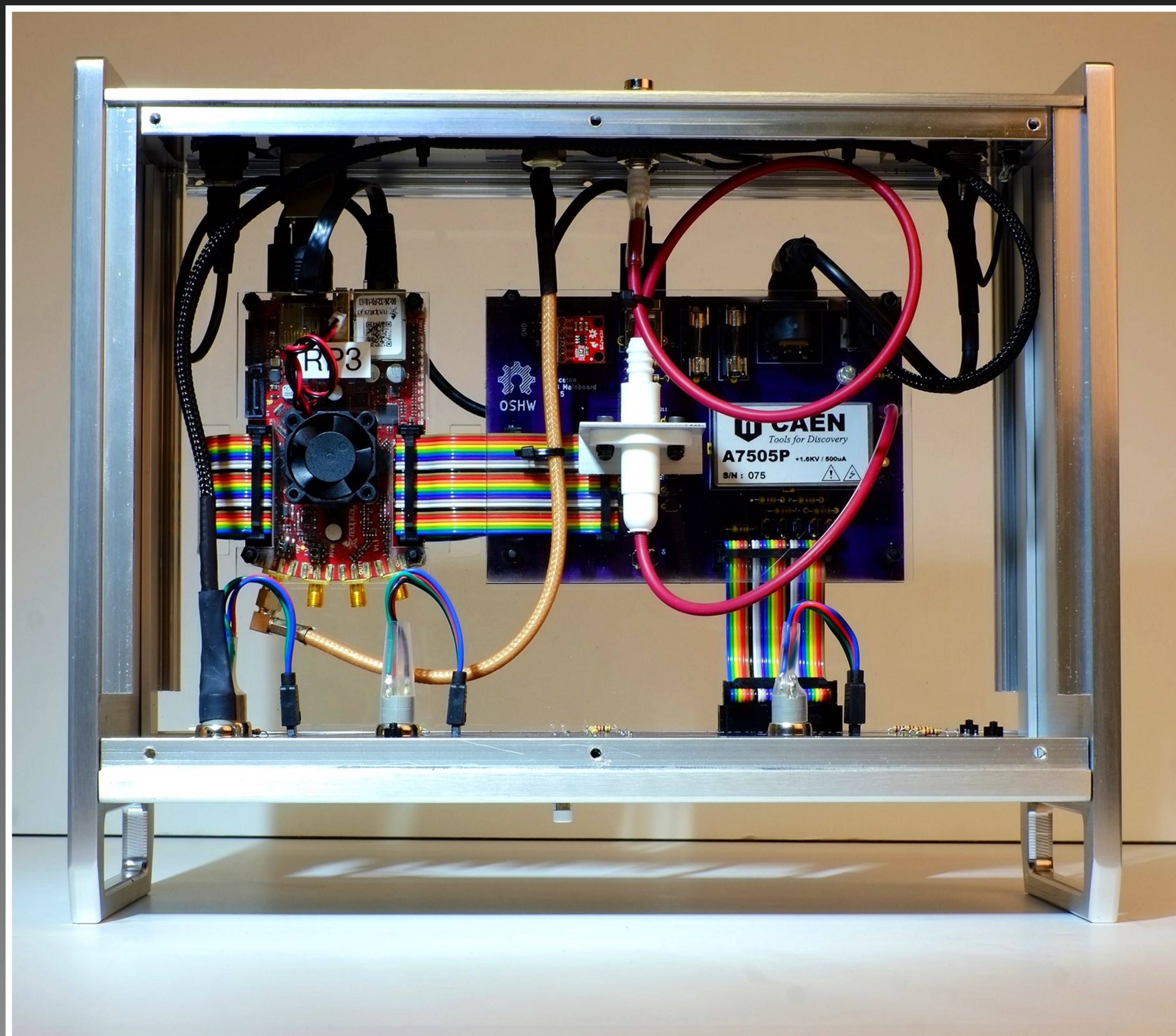
Never measure sensitive information

"Easy" to authenticate and certify

More complex observation

S. Philippe, B. Barak, and A. Glaser, "Designing Protocols for Nuclear Warhead Verification"
56th Annual INMM Meeting, July 12-16, 2015, Indian Wells, California

INFORMATION BARRIER EXPERIMENTAL



M. Goettsche, J. Schirm, and A. Glaser, “Low-resolution Gamma-ray Spectrometry for an Information Barrier Based on a Multi-criteria Template-matching Approach,” *Nuclear Instruments and Methods A,* 840, 2016, pp. 139–144

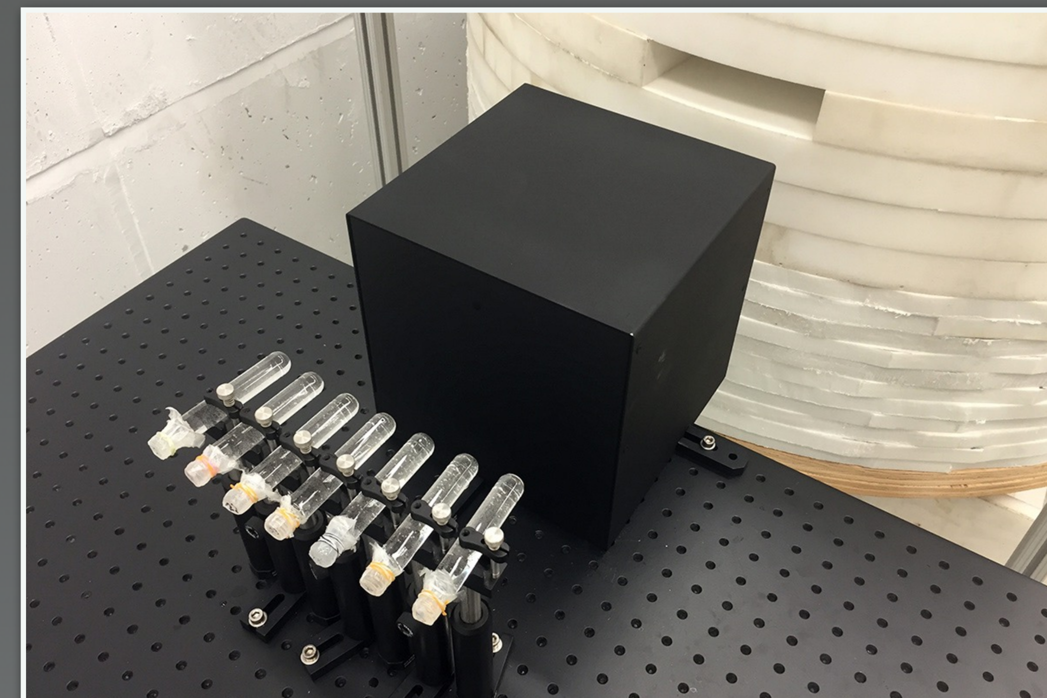
PREVENTING THE EXCHANGE OF SENSITIVE INFORMATION DURING A RADIATION MEASUREMENT

Trusted Information Barrier

Measure (but sanitize) sensitive information

“Hard” to authenticate and certify

Single-bit observation



Interactive Zero-knowledge Proof

Never measure sensitive information

“Easy” to authenticate and certify

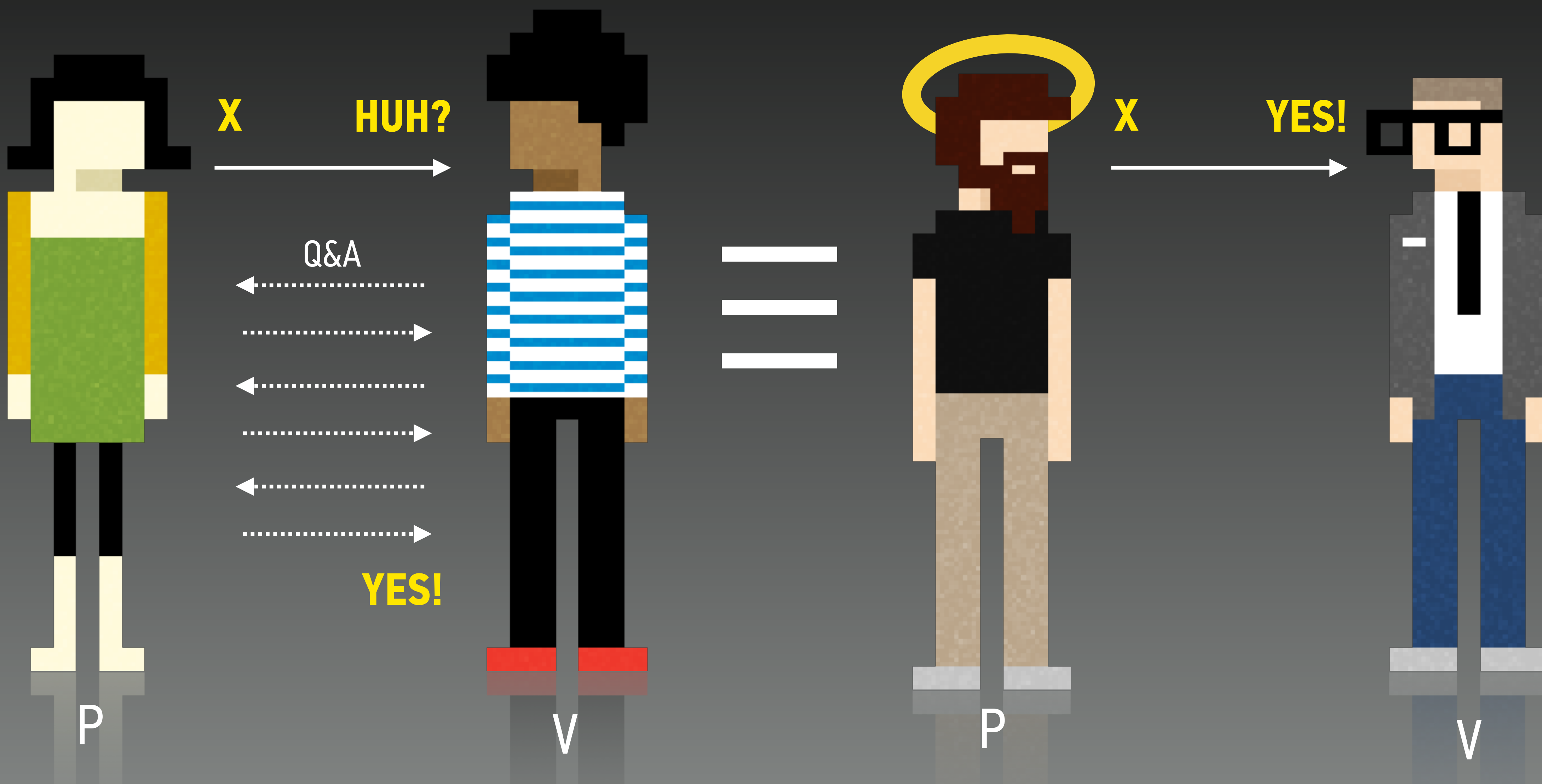
More complex observation

S. Philippe, B. Barak, and A. Glaser, “Designing Protocols for Nuclear Warhead Verification”
56th Annual INMM Meeting, July 12-16, 2015, Indian Wells, California

INTERACTIVE ZERO-KNOWLEDGE PROOFS

LOGICAL LAYER

INTERACTIVE ZERO-KNOWLEDGE PROOFS



Zero-Knowledge Proofs: The prover (P) convinces the verifier (V) that s/he knows a secret without giving anything about the secret itself away

O. Goldreich, S. Micali, A. Wigderson, "How to Play ANY Mental Game," 19th Annual ACM Conference on Theory of Computing, 1987
Graphics adapted from O. Goldreich, *Foundations of Cryptography,* Cambridge University Press, 2001; and eightbit.me

EXAMPLE

FOR AN "ILLUSTRATED PRIMER" ON ZERO-KNOWLEDGE PROOFS, SEE
blog.cryptographyengineering.com/2014/11/zero-knowledge-proofs-illustrated-primer.html

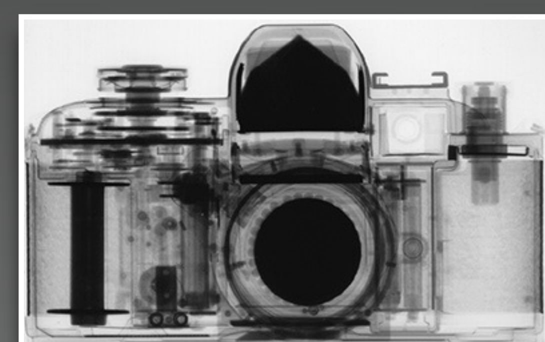
FOR A ZERO-KNOWLEDGE "SUDOKU" PROOF, SEE
www.wisdom.weizmann.ac.il/~naor/PAPERS/SUDOKU_DEMO/

PROVING THAT TWO OBJECTS ARE IDENTICAL

“THE DAY BEFORE THE INSPECTION”

1

2



3

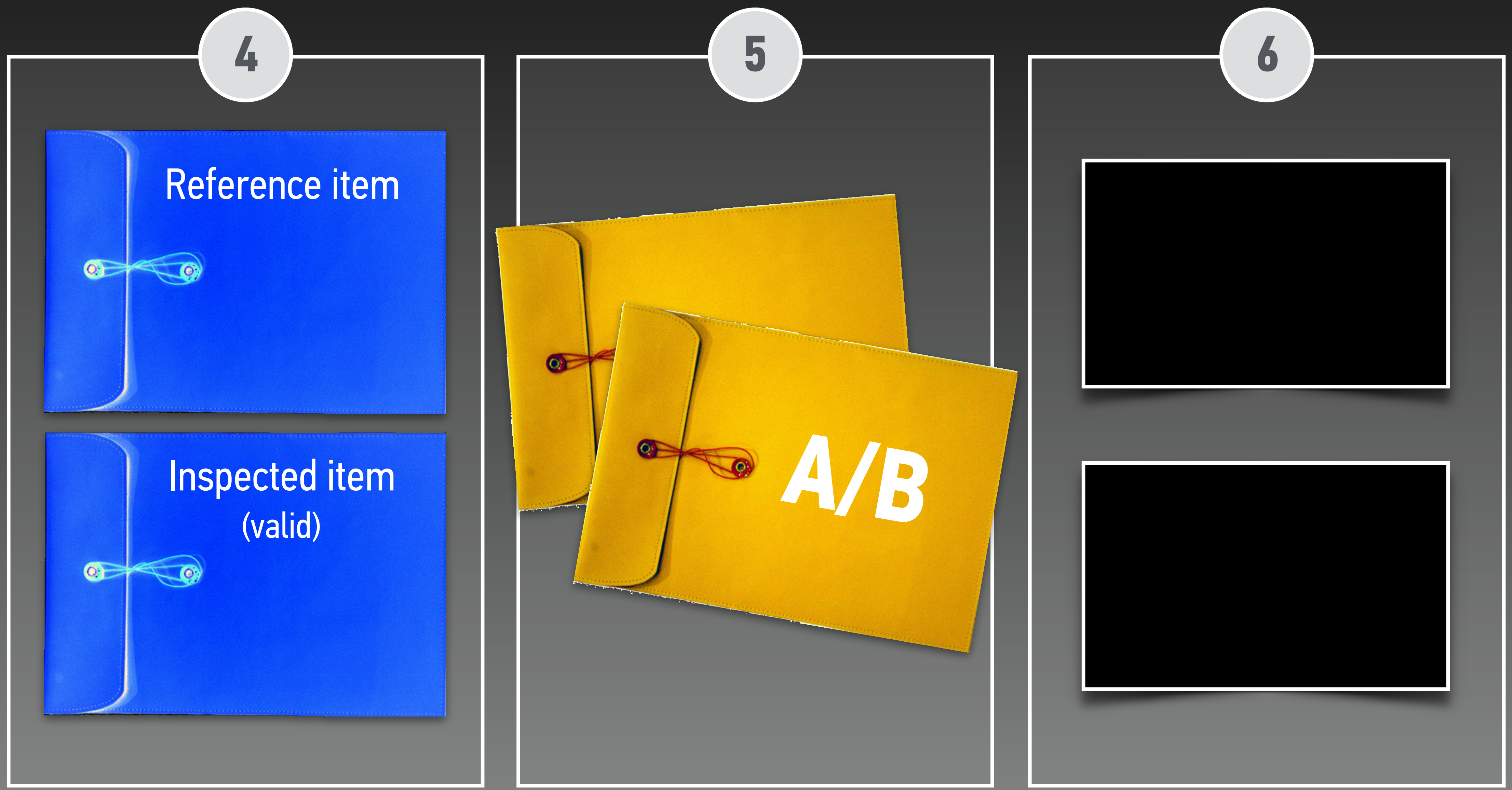
(1) Alice owns valuable objects whose design she wants to keep a secret

(2) In private, she takes a radiograph of this object on “blank film”

(3) Alice prepares two identical complements of that picture and places these complements in two sealed envelopes

PROVING THAT TWO OBJECTS ARE IDENTICAL

"THE DAY OF THE INSPECTION"



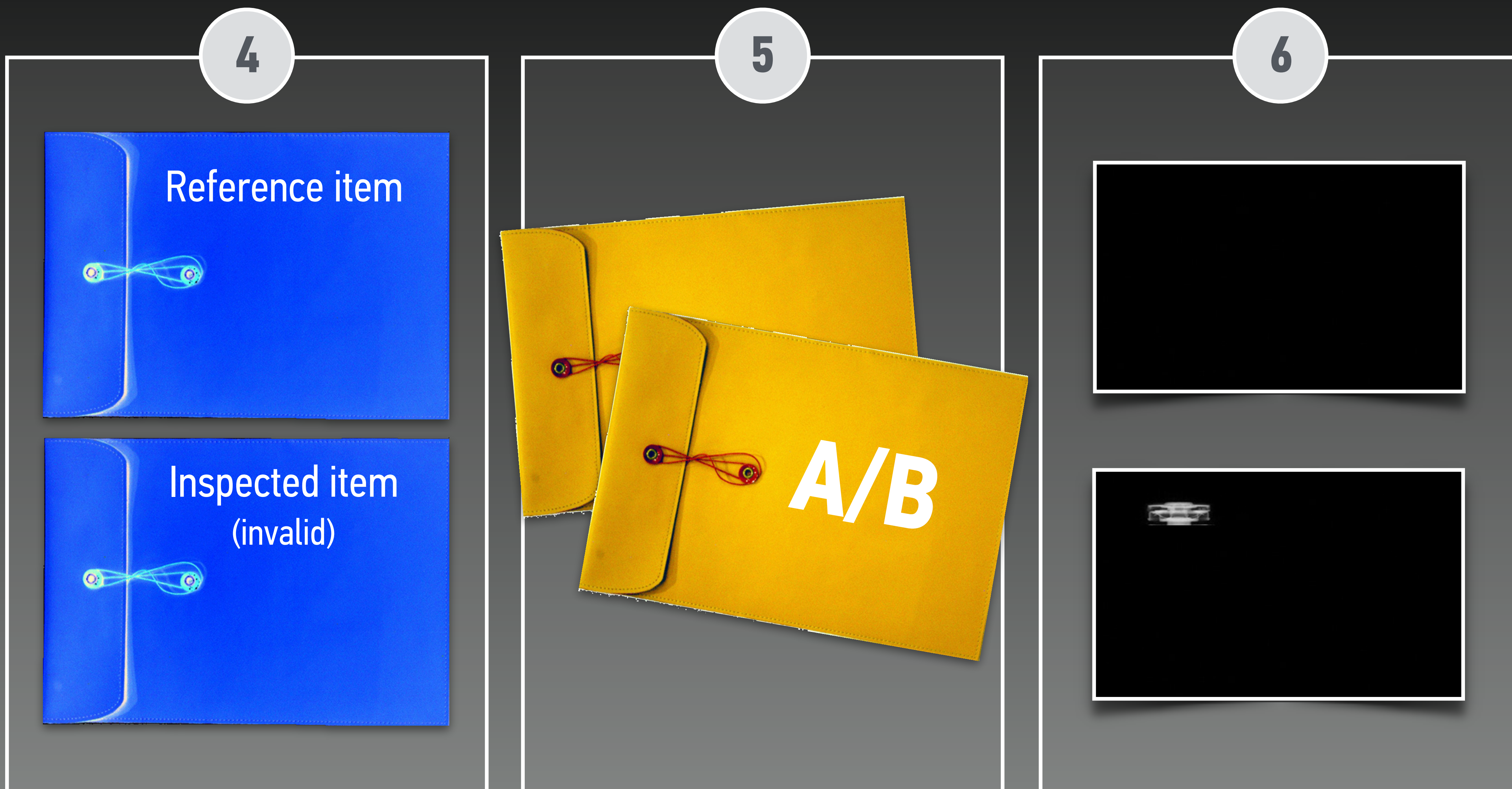
(4) At the day of the inspection, Alice presents a reference item and an item for inspection in concealed form

(5) Bob <u>randomly assigns</u> the envelopes; then, new radiographs of both items are made

(6) If Alice presents a valid item, a "flat image" is produced; if not, she risks failing the inspection (and revealing information)

PROVING THAT TWO OBJECTS ARE IDENTICAL

“THE DAY OF THE INSPECTION”



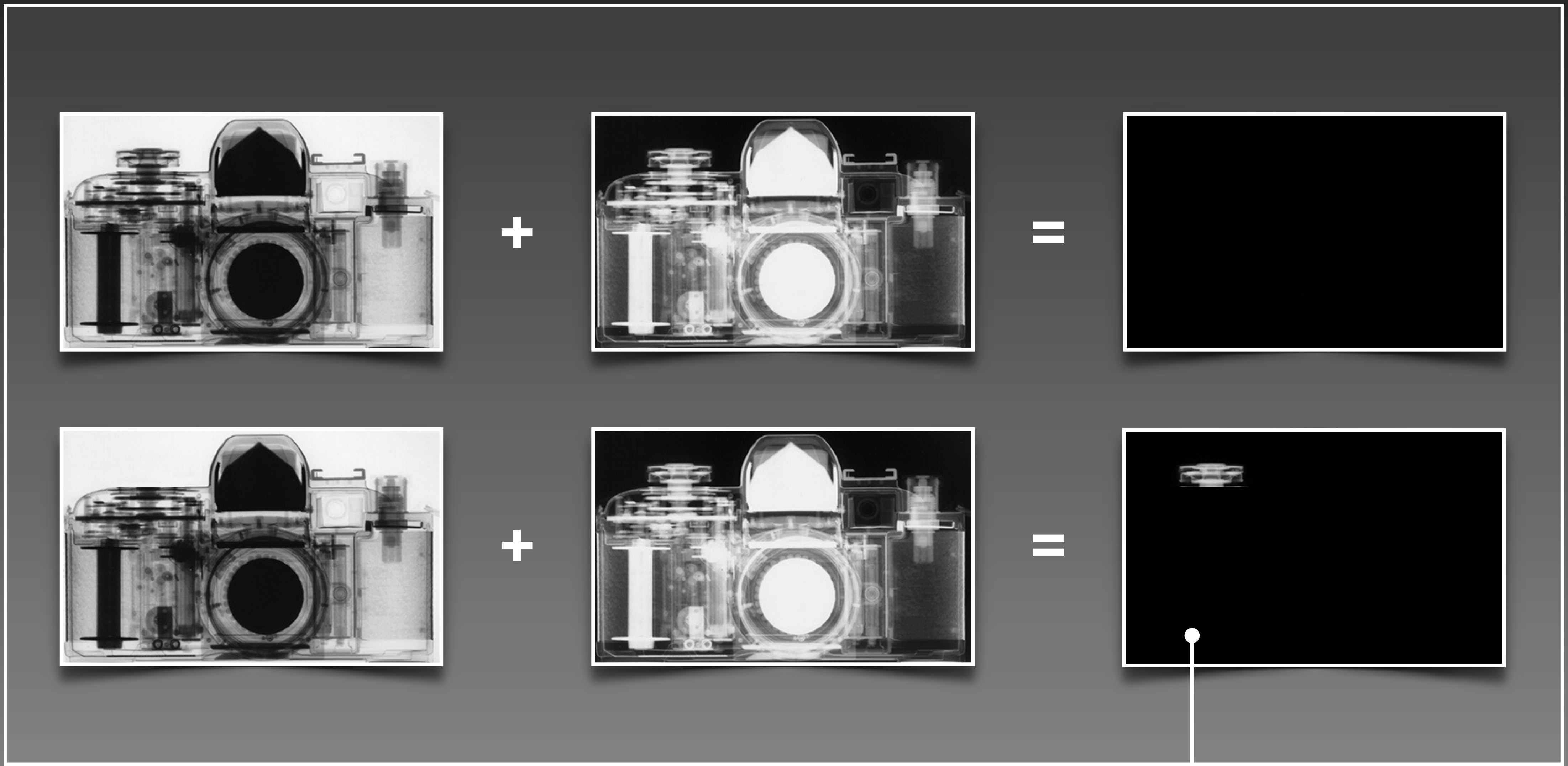
(4) At the day of the inspection, Alice presents a reference item and an item for inspection in concealed form

(5) Bob <u>randomly assigns</u> the envelopes; then, new radiographs of both items are made

(6) If Alice presents a valid item, a “flat image” is produced; if not, she risks failing the inspection (and revealing information)

PROVING THAT TWO OBJECTS ARE IDENTICAL

"THE DAY OF THE INSPECTION"



We will later introduce the maximum possible exposure as "N_{MAX}"

WHAT THE PROTOCOL ACHIEVES

COMPLETENESS

If the items are identical and both host and inspector follow the protocol,
then the inspector will accept with probability $p = 1 - (½)^n$

SOUNDNESS

If the items are different and the inspector follows the protocol,
then, no matter what the host does, the inspector will reject with probability $p \geq 1 - (½)^n$

ZERO KNOWLEDGE

As long as the host follows the protocol and presents matching items,
the inspector gains no knowledge during their interaction except for the fact that the items match

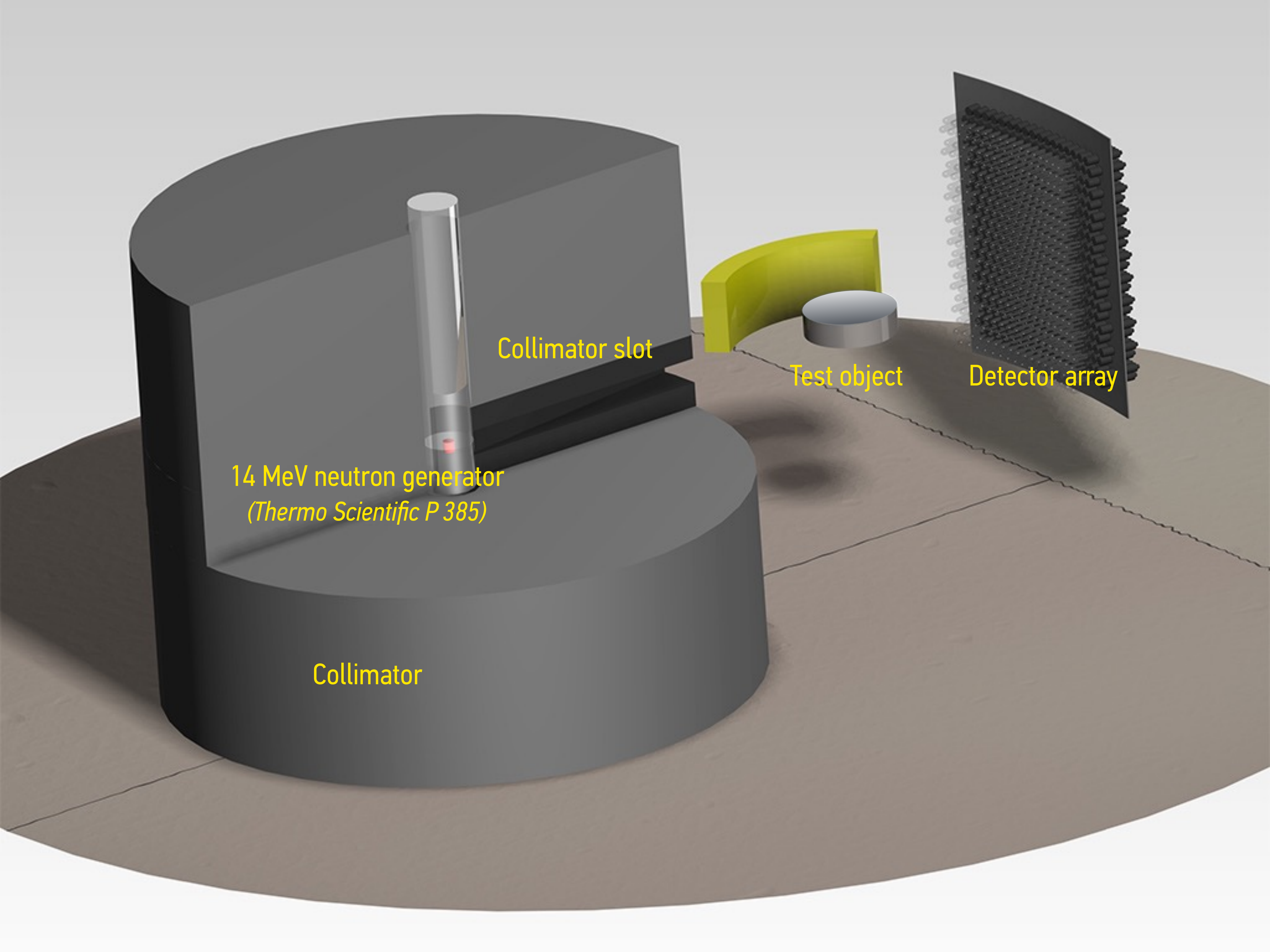
S. Philippe, B. Barak, and A. Glaser, "Designing Protocols for Nuclear Warhead Verification"
56th Annual INMM Meeting, July 12-16, 2015, Indian Wells, California

PHYSICAL ZERO-KNOWLEDGE PROOFS

WITH NON-ELECTRONIC PRELOADABLE DETECTORS

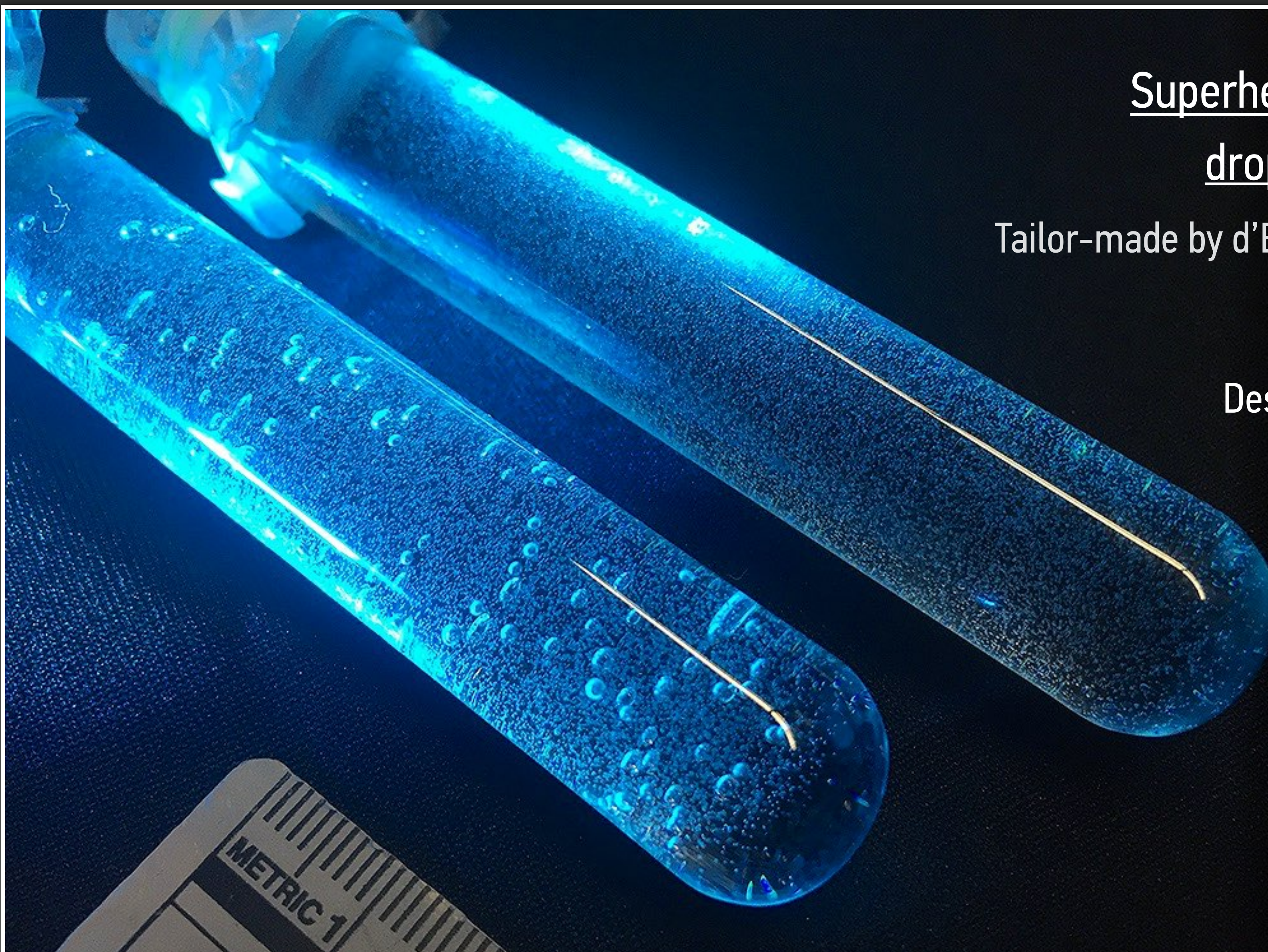
THIS BASIC IDEA HAS TRIGGERED INTEREST IN OTHER "PHYSICAL APPLICATIONS" OF ZERO-KNOWLEDGE

see, for example, B. Fisch, D. Freund, M. Naor, "Physical Zero-Knowledge Proofs of Physical Properties"
Advances in Cryptology, CRYPTO 2014, Lecture Notes in Computer Science, Volume 8617, Springer, Heidelberg, 2014


Collimator slot
Test object
Detector array
14 MeV neutron generator
(Thermo Scientific P 385)
Collimator

SUPERHEATED DROPLET DETECTORS OFFER A WAY TO IMPLEMENT THIS PROTOCOL

AND AVOID DETECTOR-SIDE ELECTRONICS



Superheated C-318 fluorocarbon (C_4F_8) droplets suspended in aqueous gel

Tailor-made by d'Errico Research Group, Yale University

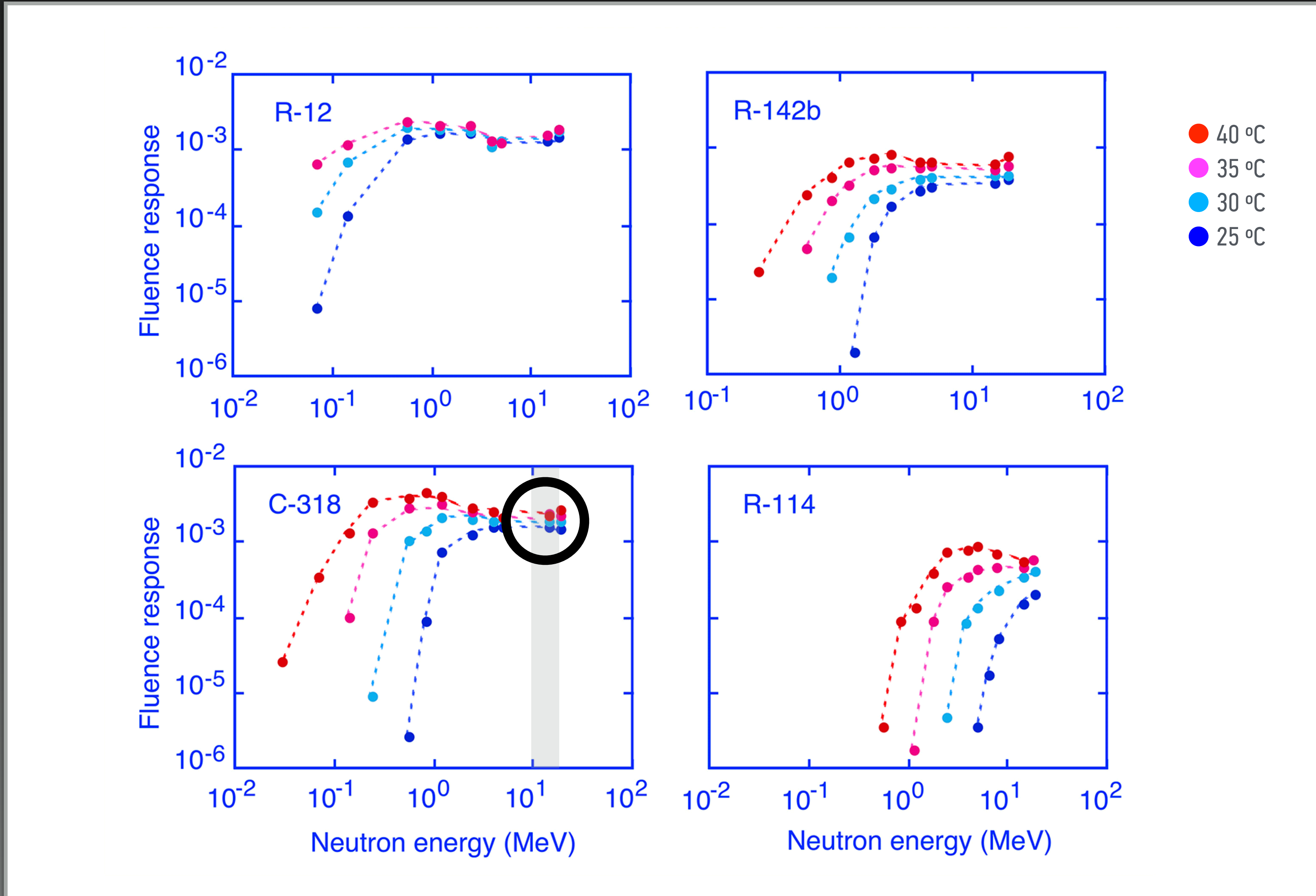
Sensitive to neutrons with $E_n > E_{min}$

Designed to be insensitive to γ-radiation

Active volume .... :	6.0 cm^3
Droplet density .... :	3500 cm^{-3}
Droplet diameter ...... :	~100 μm
Absolute Efficiency ... :	4 x 10^{-4}

FLUENCE RESPONSE

OF SUPERHEATED EMULSIONS MEASURED AS A FUNCTION OF NEUTRON ENERGY AND TEMPERATURE



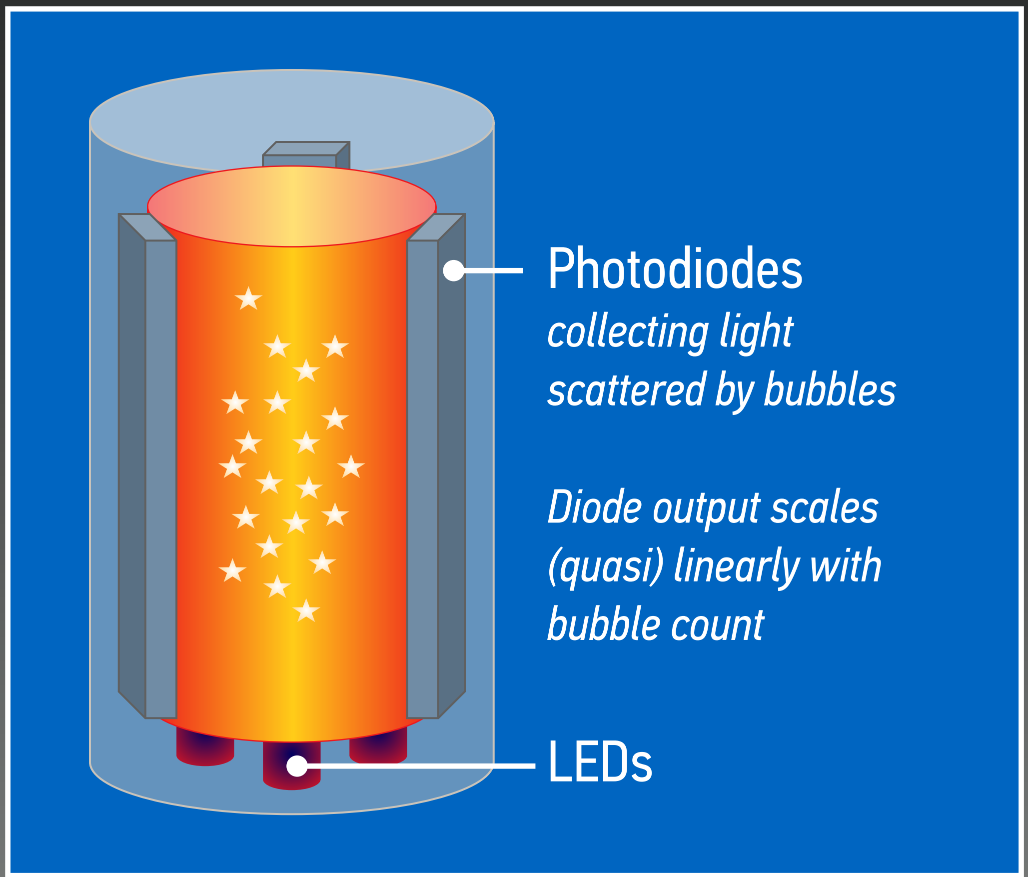
Francesco d'Errico, "Radiation Dosimetry and Spectrometry with Superheated Emulsions"
Nuclear Instruments and Methods in Physics Research B, 184 (2001), pp. 229–254

SUPERHEATED DROPLET DETECTORS

BUBBLES CAN BE COUNTED WITH A VARIETY OF TECHNIQUES

Optical readout (with camera)
Source: Bubble Technologies Industries

Volumetric readout



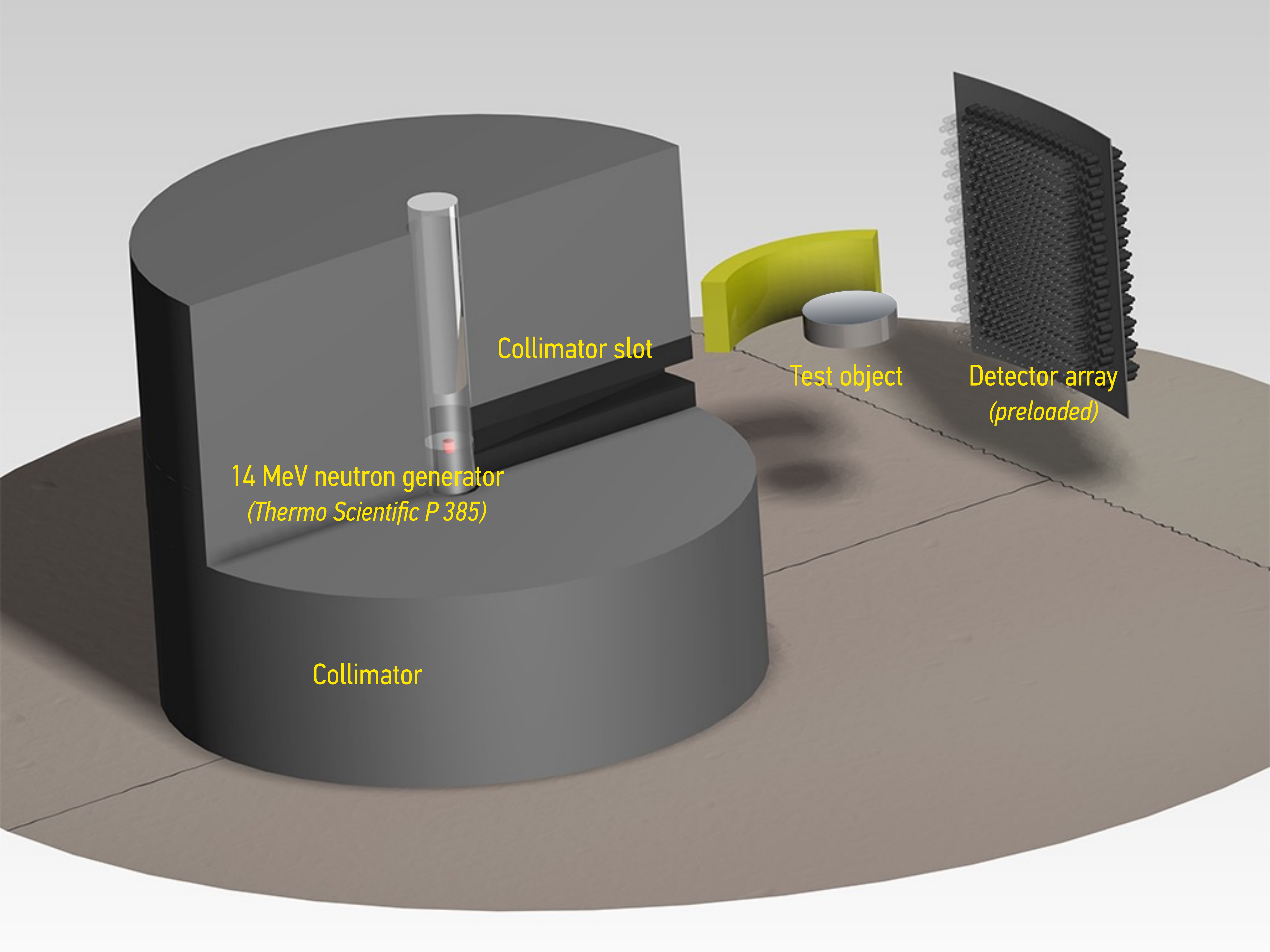
Opto-electronic readout
Adapted from: Francesco d'Errico, Yale

Detectors can be "reset" (bubbles recompressed) many times (good for R&D)

Inspector can verify functionality of detectors after inspection

RESULTS

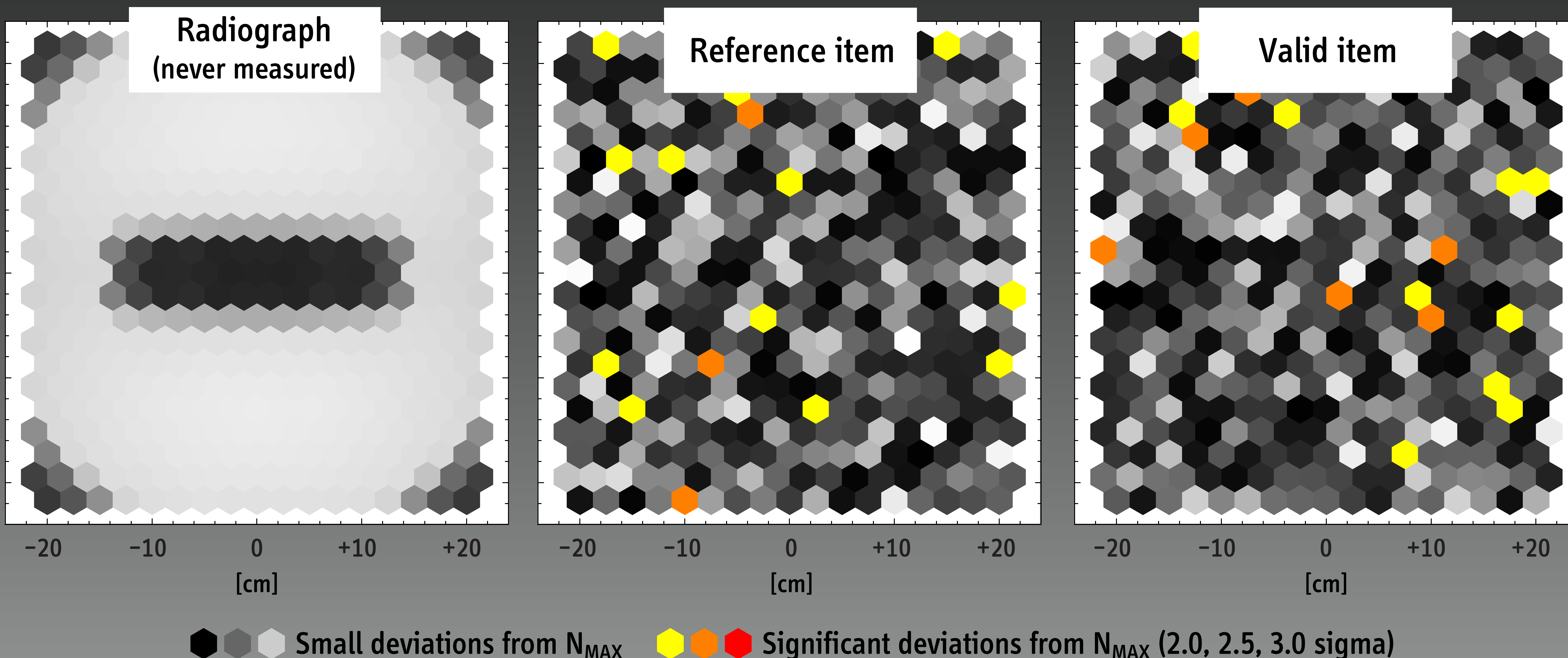
RADIOGRAPHY WITH 14-MeV NEUTRONS
(SIMULATED DATA)



Collimator slot
Test object
Detector array
(preloaded)
14 MeV neutron generator
(Thermo Scientific P 385)
Collimator

ZERO-KNOWLEDGE VERIFICATION

RADIOGRAPHY WITH 14 MeV NEUTRONS



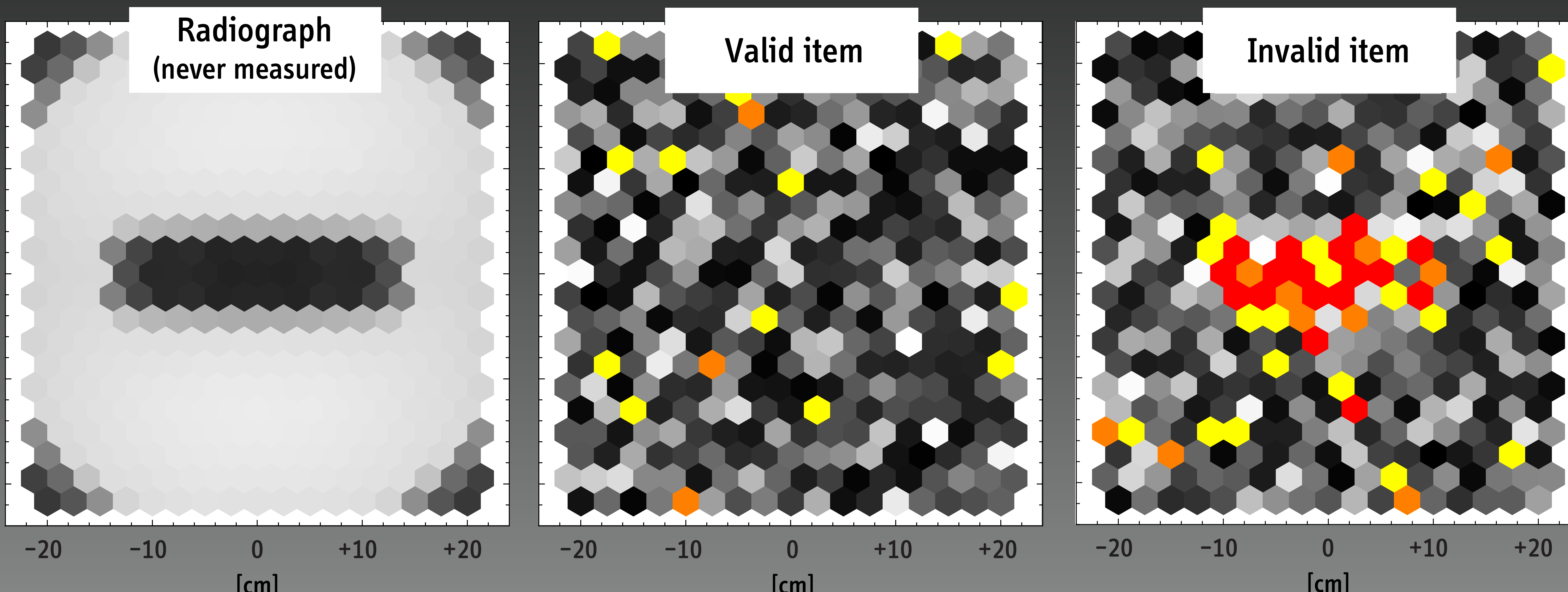
Simulated data from MCNP calculations; neutron detection energies > 10 MeV; N(max) = 5,000

A. Glaser, B. Barak, R. J. Goldston, "A Zero-knowledge Protocol for Nuclear Warhead Verification," *Nature,* 510, 26 June 2014, 497–502

ZERO-KNOWLEDGE VERIFICATION

RADIOGRAPHY WITH 14 MeV NEUTRONS

(Tungsten rings replaced by lead rings)



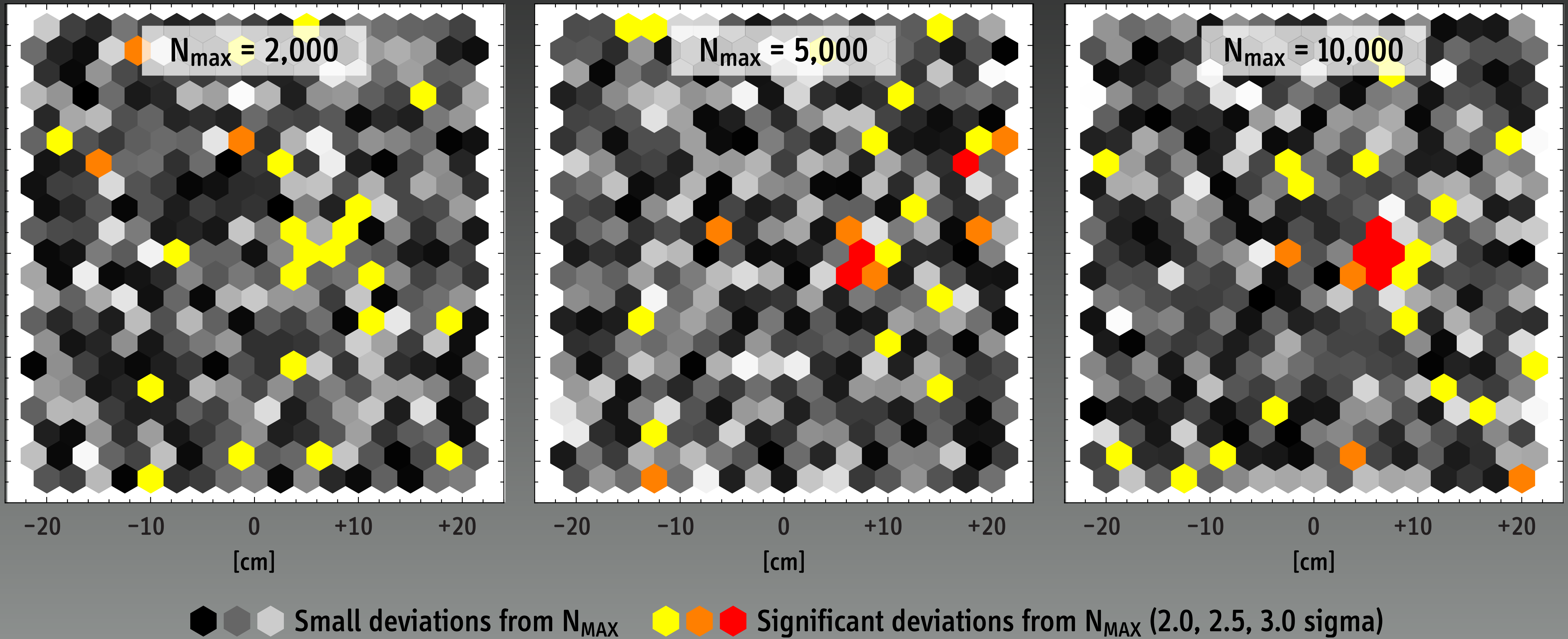
Small deviations from N_{MAX} Significant deviations from N_{MAX} (2.0, 2.5, 3.0 sigma)

Simulated data from MCNP calculations; neutron detection energies > 10 MeV; N(max) = 5,000

A. Glaser, B. Barak, R. J. Goldston, “A Zero-knowledge Protocol for Nuclear Warhead Verification,” *Nature,* 510, 26 June 2014, 497–502

ZERO-KNOWLEDGE VERIFICATION

LOCAL TUNGSTEN DIVERSION (540 GRAMS)



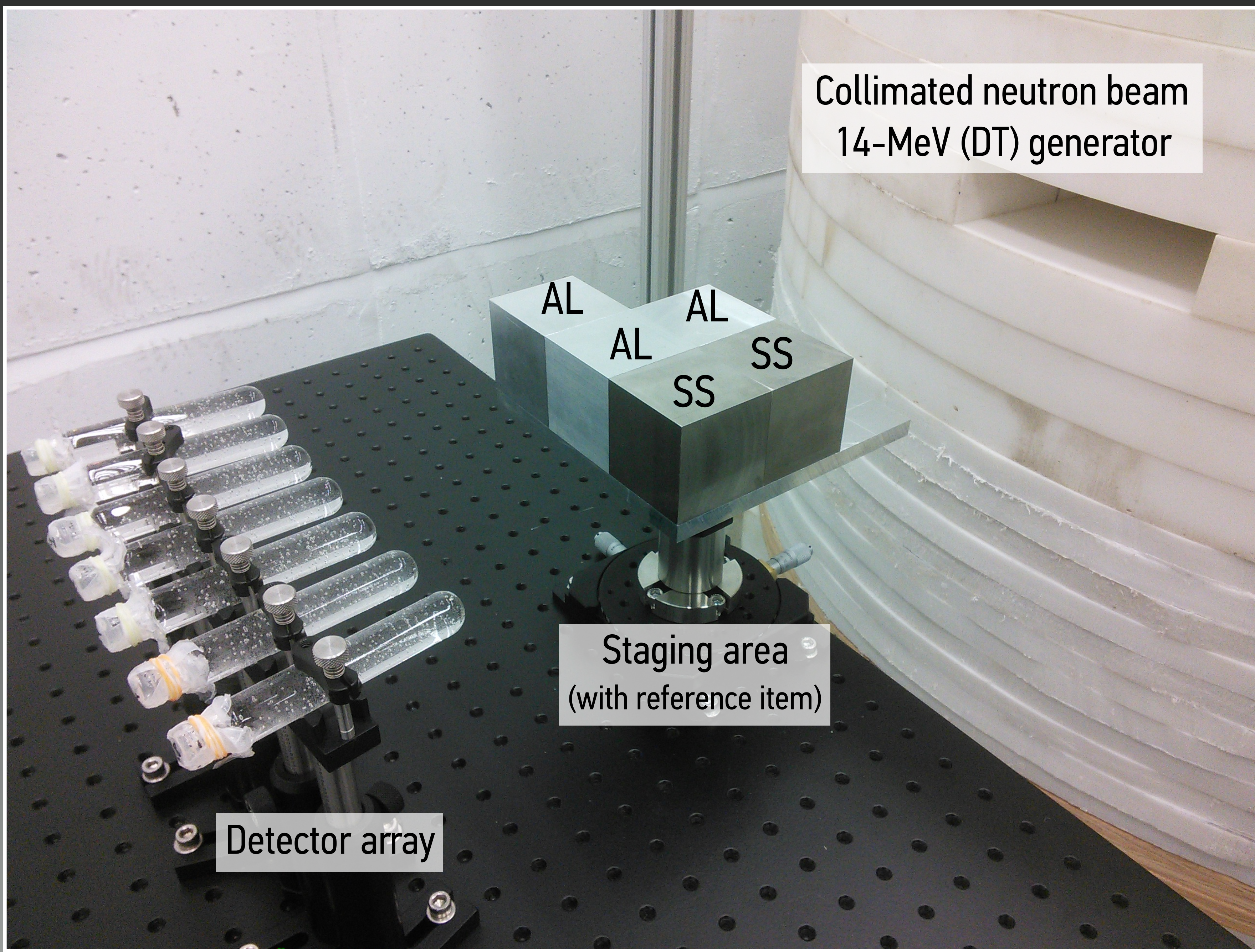
543 grams of tungsten removed from outer ring of test object; simulated data from MCNP calculations; neutron detection energies > 10 MeV
A. Glaser, B. Barak, R. J. Goldston, "A Zero-knowledge Protocol for Nuclear Warhead Verification," *Nature,* 510, 26 June 2014, 497–502

EXPERIMENTAL RESULTS

The Conjurer, Hieronymus Bosch, 1502

EXPERIMENTAL SETUP AND SCENARIO

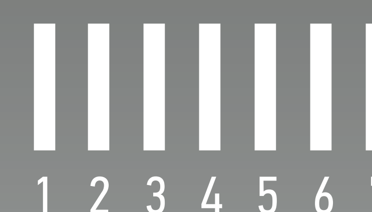
WE WISH TO IDENTIFY CASES IN WHICH THE CUBE PATTERN HAS BEEN ALTERED
WITHOUT GAINING ANY INFORMATION ABOUT THE CONFIGURATION IN CASES WHERE IT HAS NOT



Reference item consists of a combination of 2-inch cubes (aluminum and stainless steel)

Reference item

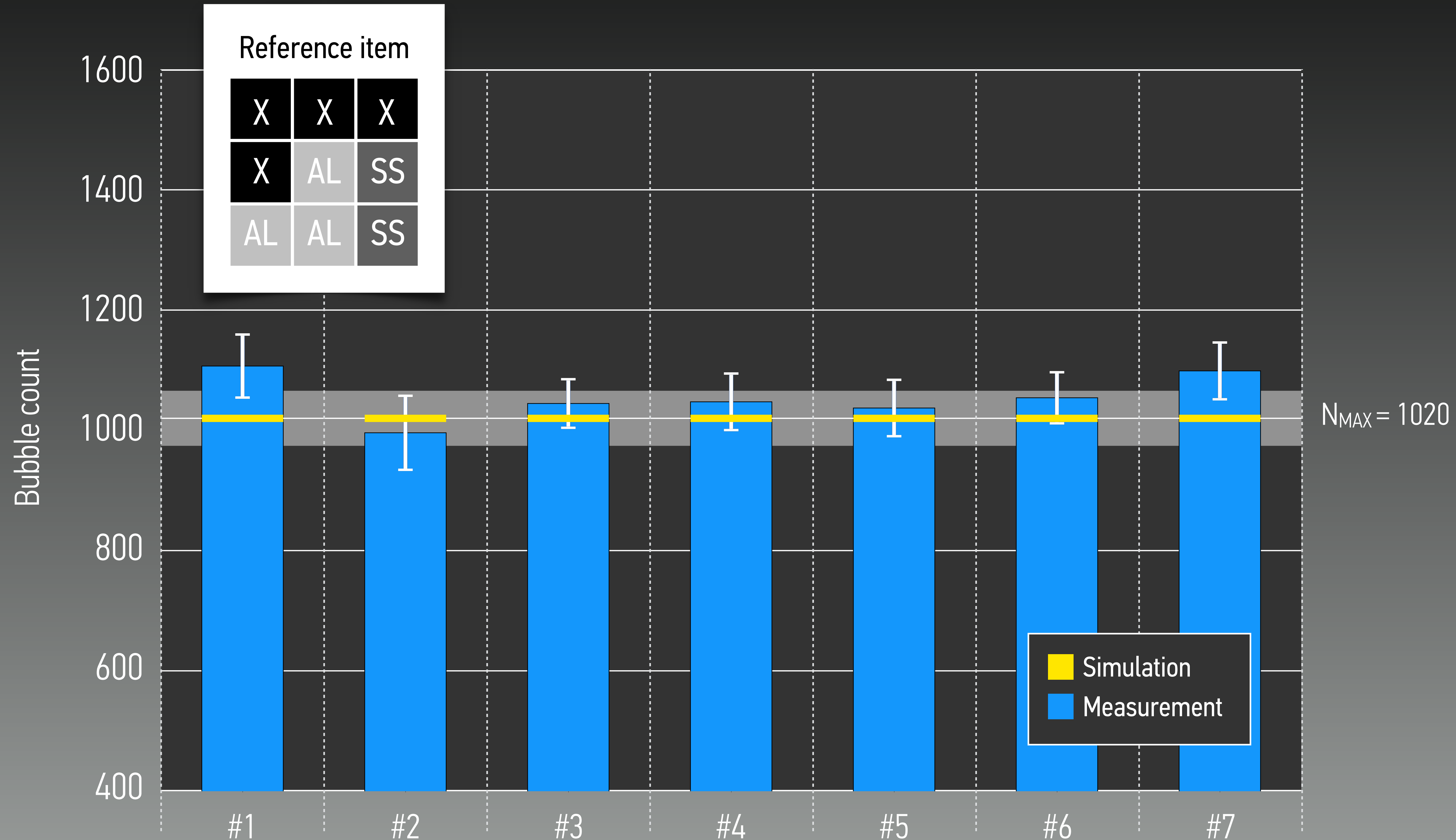
X	X	X
X	AL	SS
AL	AL	SS



Detector positions

EXPERIMENTAL RESULTS

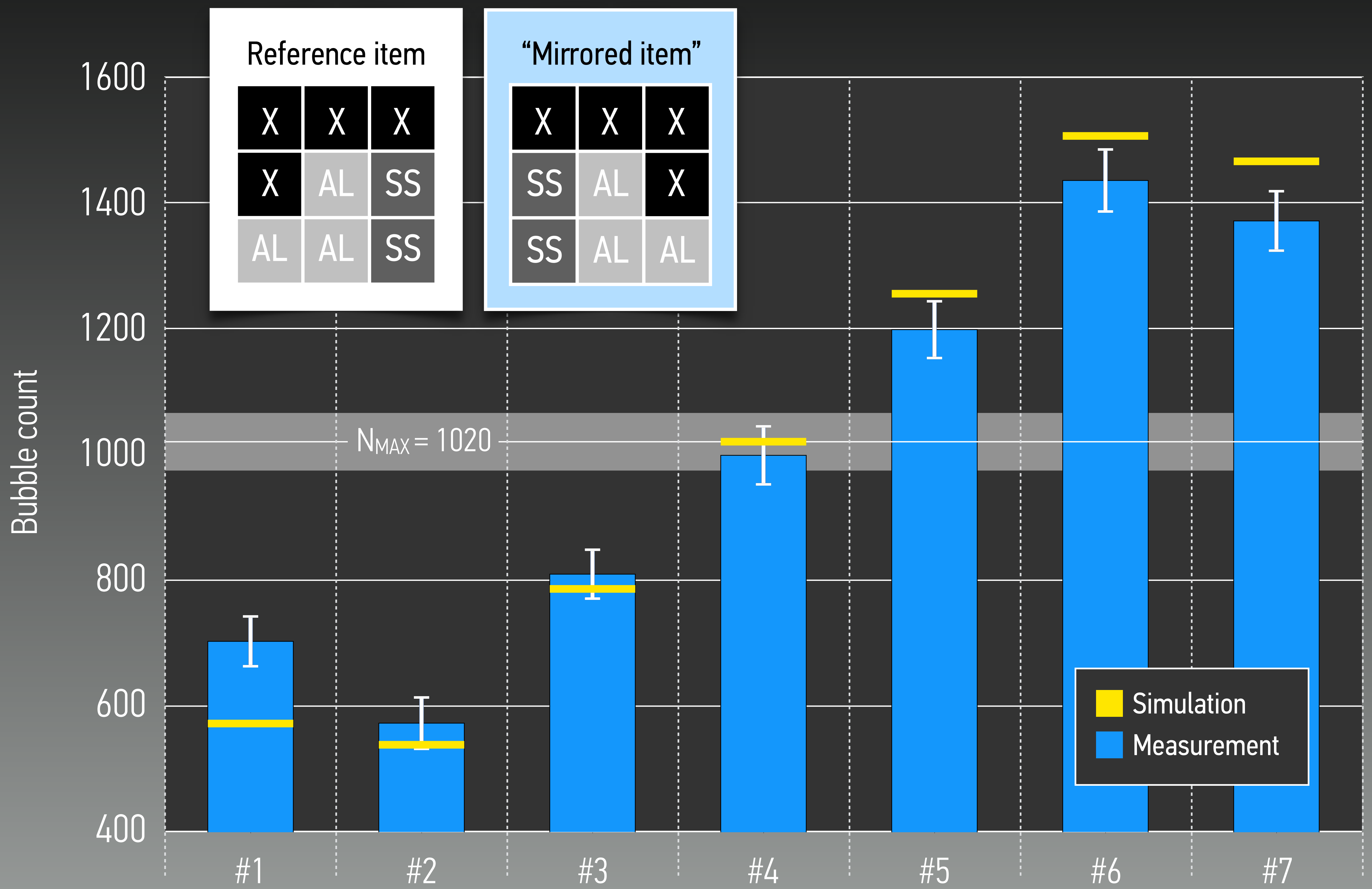
(VALID ITEM)



S. Philippe, R. J. Goldston, A. Glaser and F. d'Errico, Nature Communications, September 2016, www.nature.com/articles/ncomms12890

EXPERIMENTAL RESULTS

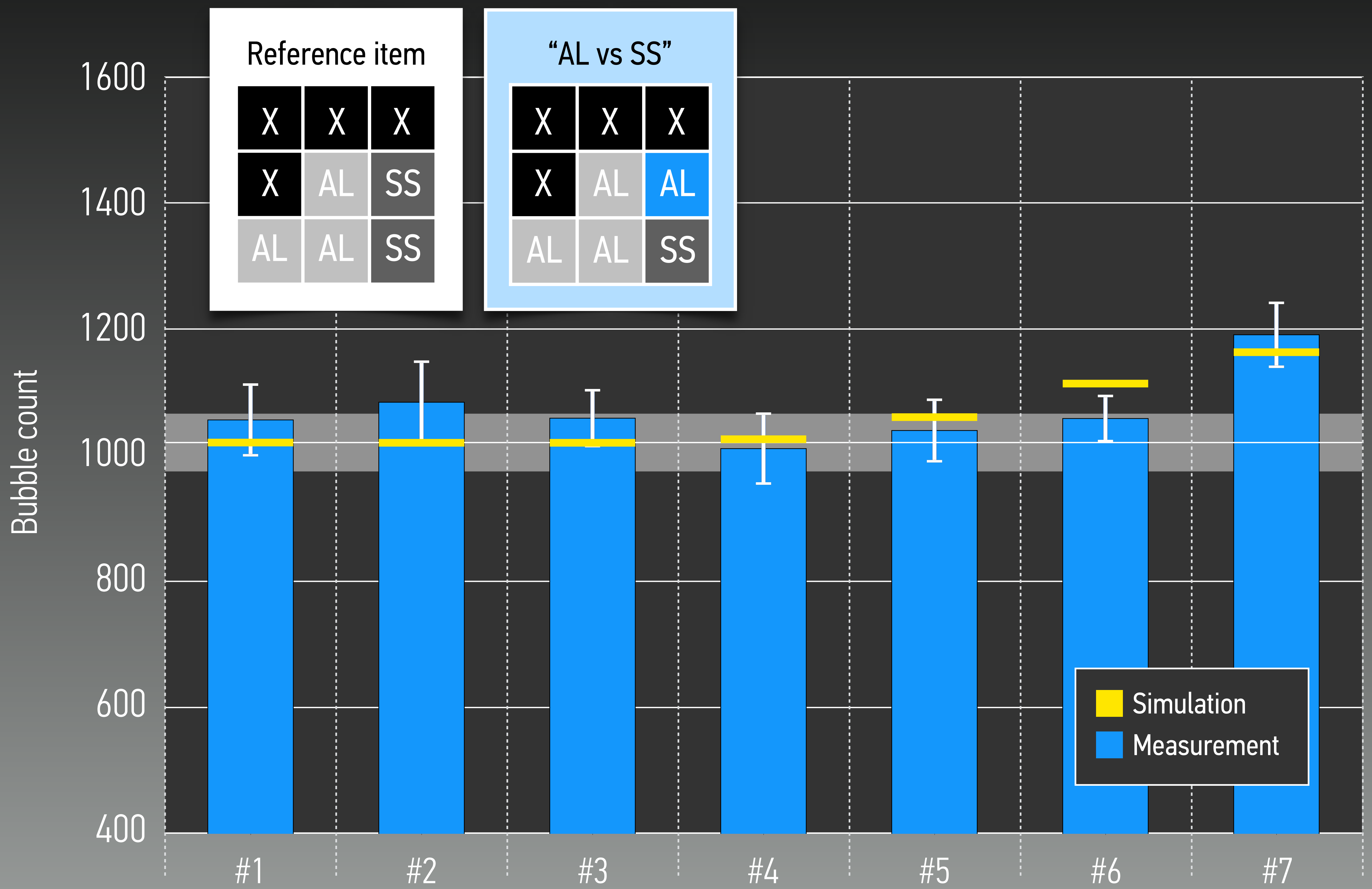
(A DRASTIC CHANGE)



S. Philippe, R. J. Goldston, A. Glaser and F. d'Errico, Nature Communications, September 2016, www.nature.com/articles/ncomms12890

EXPERIMENTAL RESULTS

(A SMALLER CHANGE)

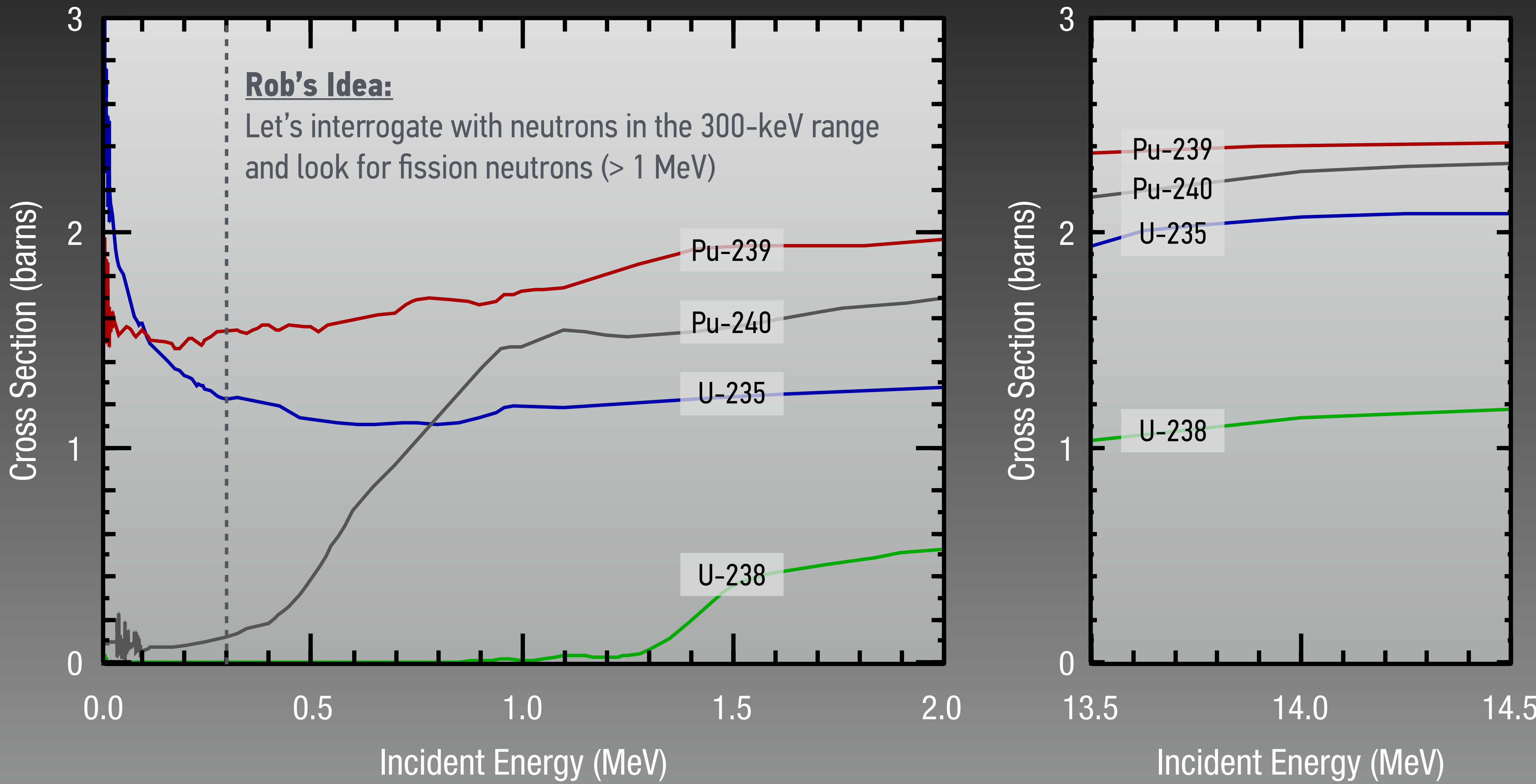


S. Philippe, R. J. Goldston, A. Glaser and F. d'Errico, Nature Communications, September 2016, www.nature.com/articles/ncomms12890

WHAT'S NEXT?

FISSION CROSS SECTIONS

OF THE MAIN URANIUM AND PLUTONIUM ISOTOPES



Source: Evaluated Nuclear Data File (ENDF), www-nds.iaea.org/exfor/endf.htm

R. J. Goldston et al., "Zero-knowledge Warhead Verification: System Requirements and Detector Technologies," 55th INMM Meeting, 2014

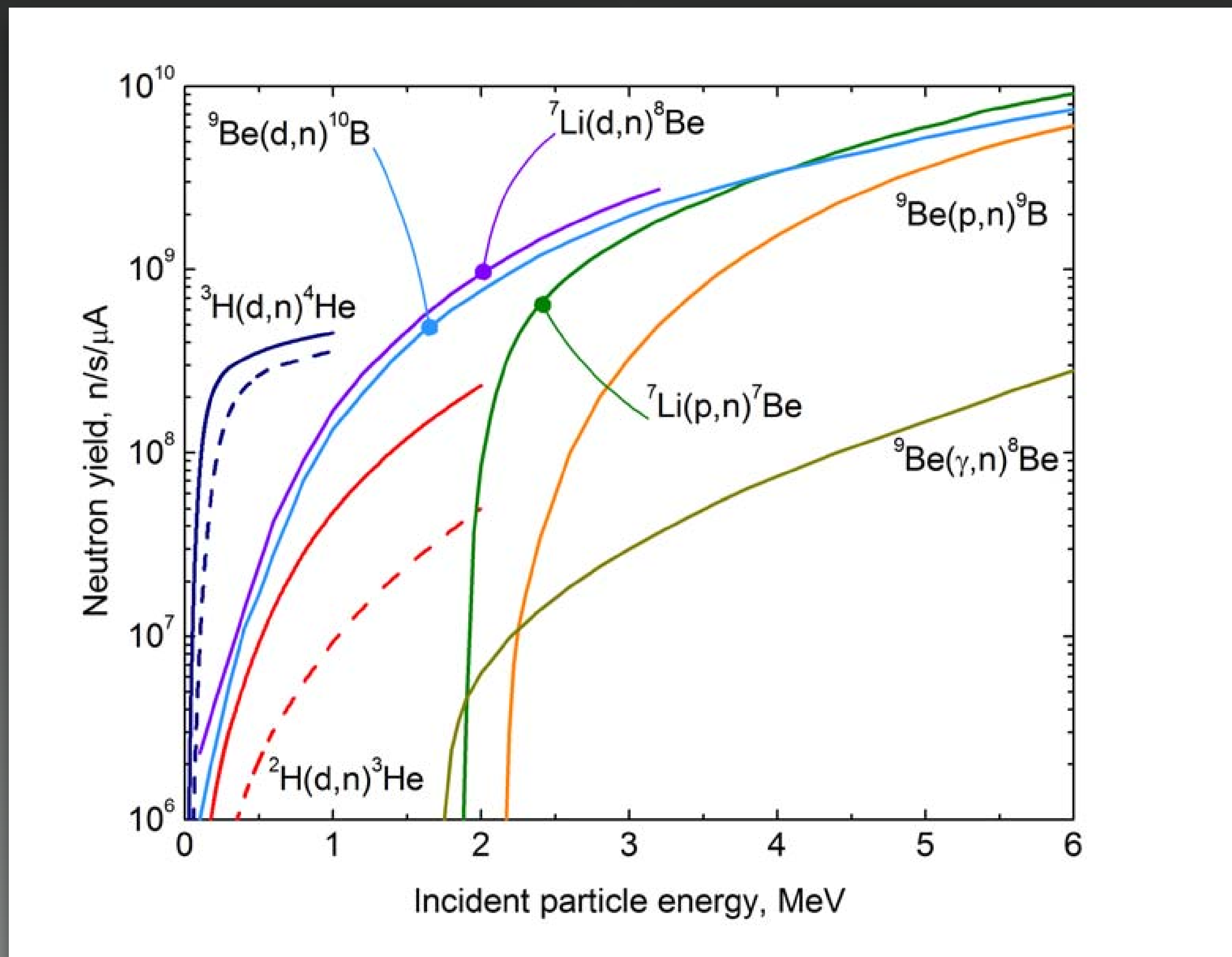
“TWO-COLOR INTERROGATION”

INTERROGATION WITH NEUTRONS FROM (p-^{7}Li) REACTION

(tuned to ~300 keV energy cutoff)

A STRONG 300-keV NEUTRON SOURCE

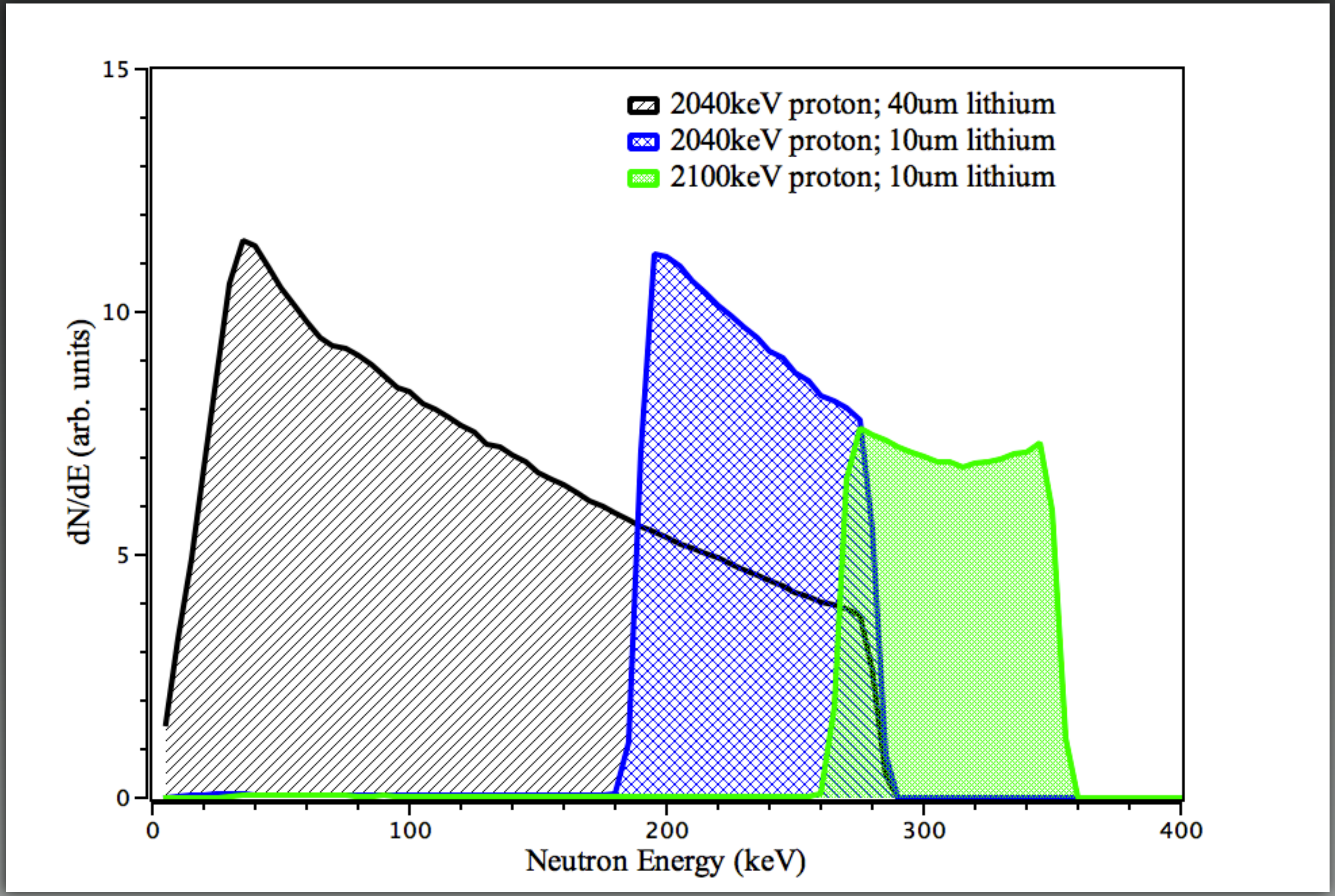
TOTAL NEUTRON YIELD CURVES FOR SELECTED (THRESHOLD) REACTIONS



David L. Chichester, *Production and Applications of Neutrons Using Particle Accelerators*
INL/EXT-09-17312, Idaho National Laboratory, November 2009

SIMULATED p-Li NEUTRON SOURCE

SPECTRUM CAN BE TAILORED BY ADJUSTING THE INCIDENT PROTON ENERGY
AND THE THICKNESS OF THE LITHIUM TARGET



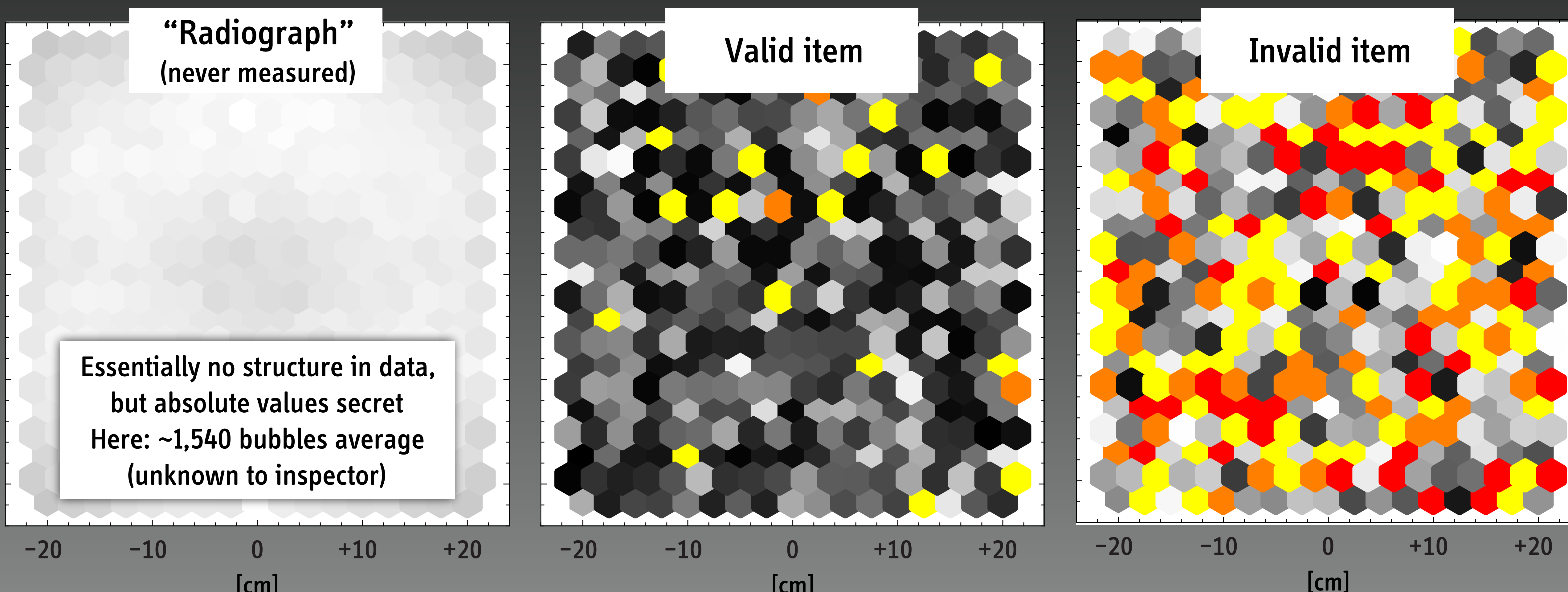
Source: SIMLiT simulations by Yan Jie, Princeton University

BARE PLUTONIUM SPHERE

8.00 cm DIAMETER SPHERE, WEAPON-GRADE PLUTONIUM

Test item based on BeRP ball, see J. Mattingly and D. J. Mitchell, *Applied Radiation and Isotopes*, 70 (2012), 1136–1140

(Isotopic shift from 93.7% to 81.2% Pu-239)



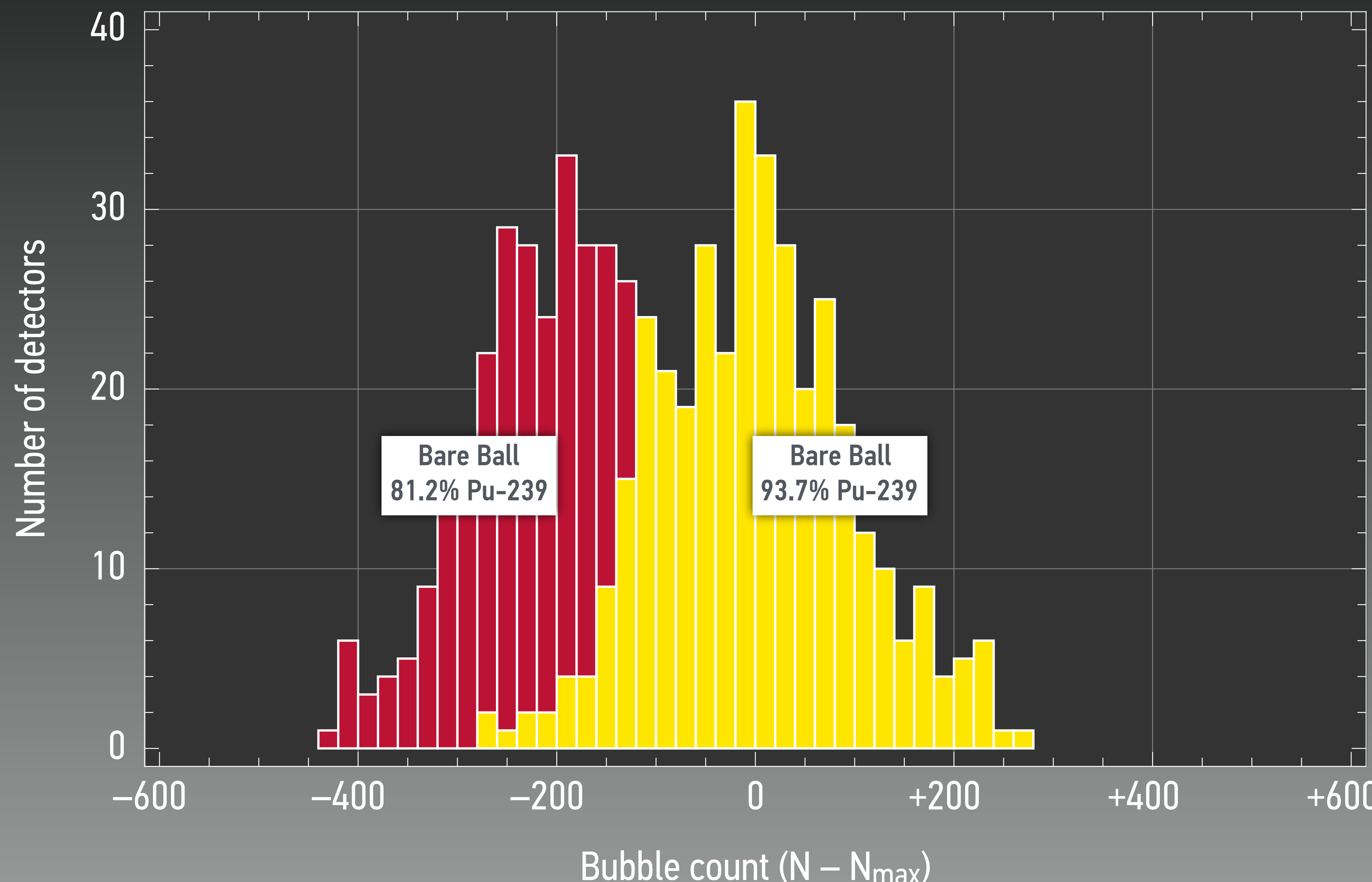
Small deviations from N_{MAX} Significant deviations from N_{MAX} (2.0, 2.5, 3.0 sigma)

Simulated data from MCNP6 calculations, neutron detection energies > 500 keV
N(max) = 10,000, i.e., 6–7 times higher than actual values from test item

BARE PLUTONIUM SPHERE

8.00 cm DIAMETER SPHERE, WEAPON-GRADE PLUTONIUM

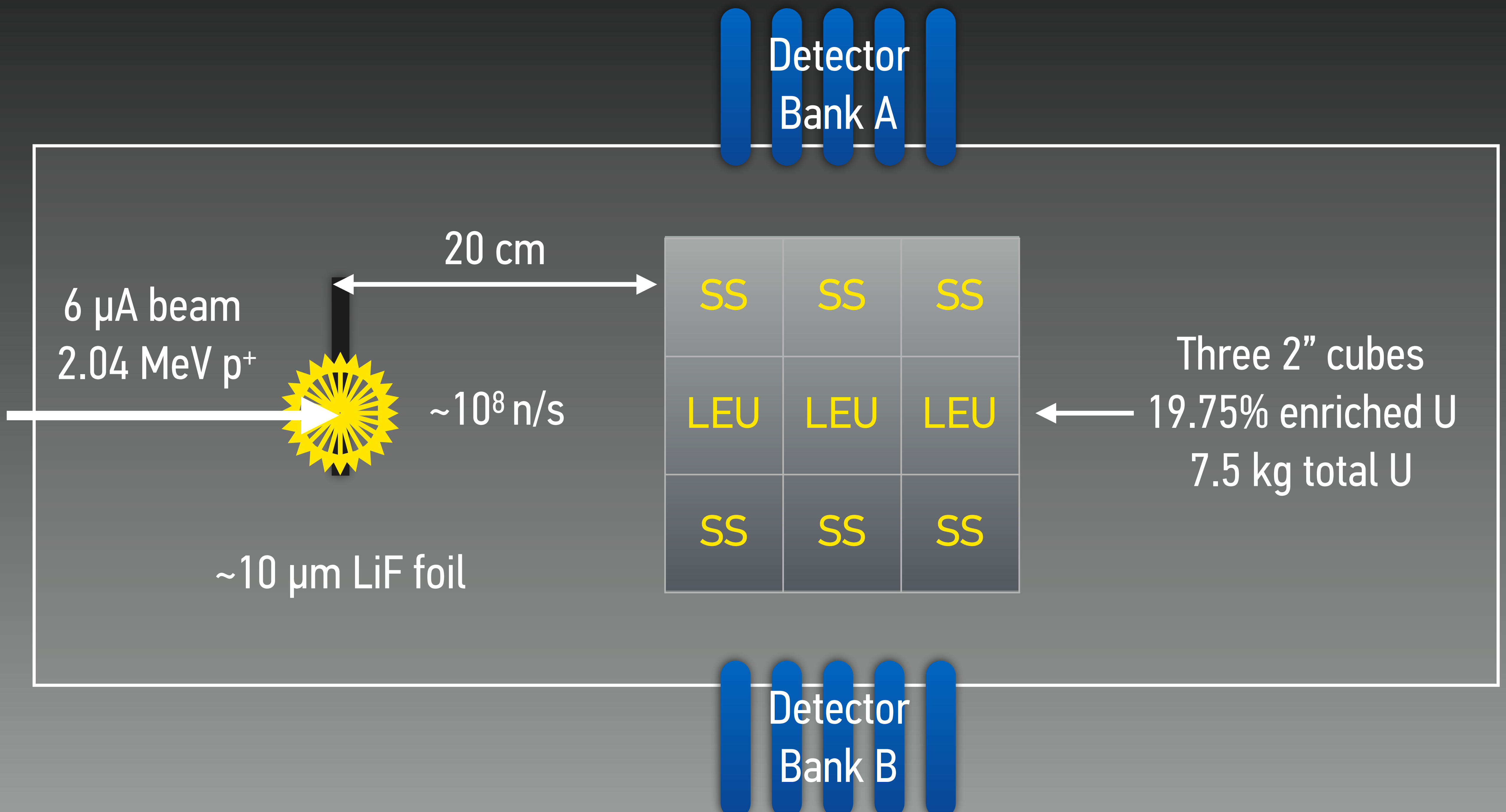
Test item based on BeRP ball, see J. Mattingly and D. J. Mitchell, *Applied Radiation and Isotopes,* 70 (2012), 1136–1140



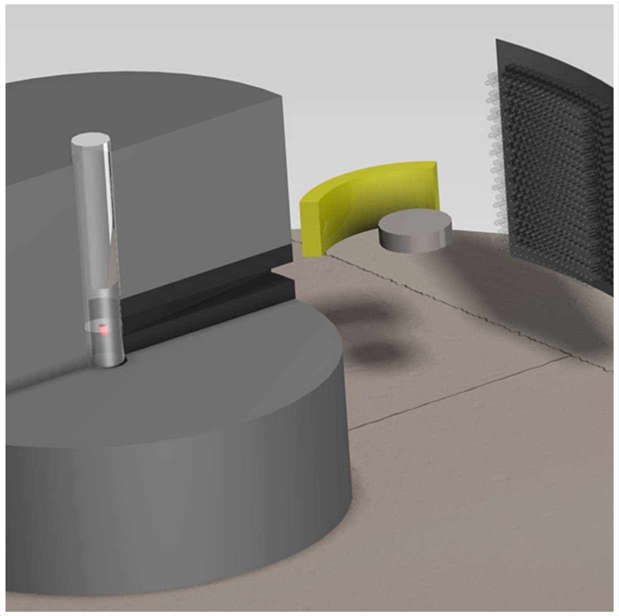
MCNP6 simulations, N(max) = 10,000

A TWO-COLOR SETUP AT TUNL?

USING 2 MEV PROTONS FROM TANDEM ON LIF TARGET



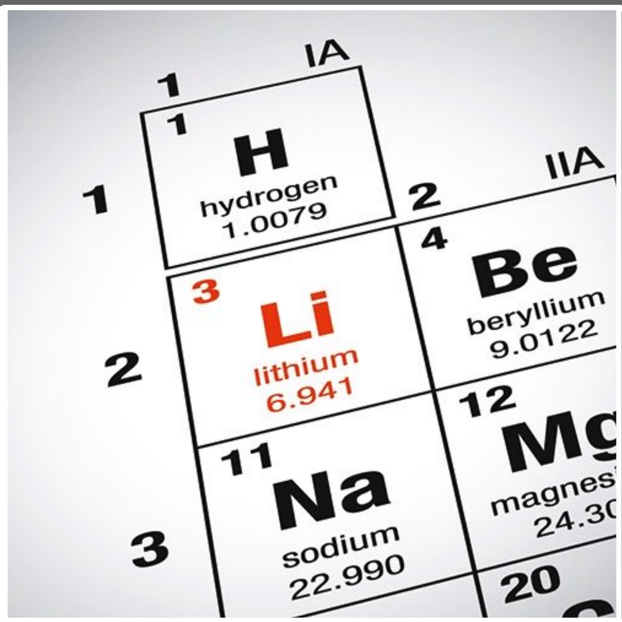
CONCLUSION AND OUTLOOK



"ONE-COLOR" SETUP

Neutron transmission radiography using high-energy (14 MeV) neutrons is effective in detecting geometric and elemental differences

Distinguishing isotopic differences can be more challenging because relevant 14-MeV total and fission cross sections can be similar for some important elements (esp. for Pu-239 vs Pu-240)



"TWO-COLOR" SETUP

Fission signatures triggered by ~ 300-keV neutrons are extremely sensitive to isotopic differences (and also to differences in geometry)

Combine with 14-MeV transmission radiography

Needed for experimental demonstration: Intense 2-MeV proton source

Photo: Mikhail Klimentyev/AP

ACKNOWLEDGEMENTS

PRINCETON AND PPPL

Andrew Carpe
Charles Gentile
Robert J. Goldston
Sébastien Philippe
Yan Jie

ELSEWHERE

Boaz Barak, Microsoft Research New England / Harvard University
Francesco d'Errico, Yale University
Margarita Gattas-Sethi, Yale University

RESEARCH SUPPORTED BY

Global Zero
MacArthur Foundation
Carnegie Corporation of New York
U.S. Department of State
National Nuclear Security Administration, U.S. Department of Energy

PRINCETON UNIVERSITY | NUCLEAR FUTURES | LAB